

网络系统管理员实战宝典

张俊斌　刘增杰　编著



Windows网络系统管理员必须掌握的网络管理技能

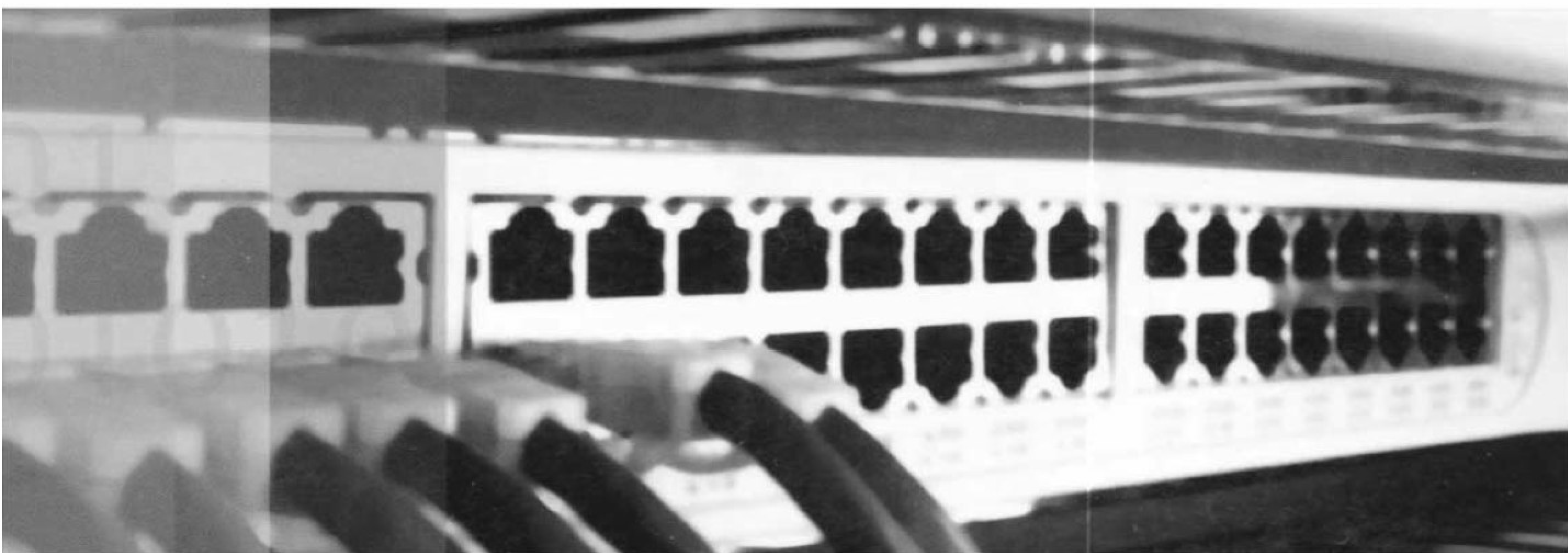
方案分析设计、网络设备、单机维护、服务器搭建和网络管理

理论＋技巧＋实战完整结合

清华大学出版社

Windows 网络系统管理员实战宝典

张俊斌　刘增杰　编著



清华大学出版社
北　京

内 容 简 介

本书主要介绍的是针对中小型企业的网络管理、维护、设备调试和服务配置等技术。全书分 20 章，内容涉及网络管理概述、单机故障维护、路由交换技术、企业级服务器配置管理技术、OA 办公自动化系统实施、网络管理平台及防火墙和 VPN 等安全技术的实施等。通过本书的学习，读者可以比较全面地掌握常备的网络管理技术。书中在讲解各个知识模块时，主要以实际操作案例的方式做引导，使读者在学习时能够了解该知识在实际网络工程、网络管理中的用途。为了使读者能够快速地掌握操作技能，本书在理论介绍方面采用了概述总结的方式，通过编者自身对技术的认识进行直观的描述，能够避免读者学习繁杂理论知识的枯燥。

本书内容丰富全面，图文并茂，深入浅出，便于读者能理解网络管理的精髓，并能解决实际生活或工作中的问题，真正做到知其然更知其所以然。

本书适用于对中小型企业管理感兴趣的零基础读者；计算机网络技术、网络工程、网络安全相关专业的学生；具有一定的网络基础知识，熟悉网络路由交换技术和网络服务器技术，能够实现简单网络搭建，对网络管理技术、网络安全技术感兴趣的工程师。

图书在版编目（CIP）数据

Windows 网络系统管理员实战宝典/张俊斌，刘增杰编著.—北京：清华大学出版社，2012.8

ISBN 978-7-302-28957-9

Ⅰ.①W…　Ⅱ.①张…②刘…　Ⅲ.①Windows 操作系统　Ⅳ.①TP316.7

中国版本图书馆 CIP 数据核字（2012）第 111539 号

责任编辑：夏非彼
封面设计：王　翔
责任校对：李金平
责任印制：

出版发行：清华大学出版社
　　网　　址：http://www.tup.com.cn，http://www.wqbook.com
　　地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
　　社 总 机：010-62770175　　**邮　　购**：010-62786544
　　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　　质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：190mm×260mm　　**印　　张**：43.25　　**字　　数**：1107 千字
版　　次：2012 年 8 月第 1 版　　**印　　次**：2012 年 8 月第 1 次印刷
印　　数：1~4000
定　　价：79.80 元

产品编号：044632-01

前　　言

随着网络技术的发展，中小型企业对于网络的管理与安全越来越重视，因此很多企业希望能招聘到有较高技术水平、较强实践能力的工程师。面对这种社会需求，很多学校也开设了网络管理或网络安全课程，但是其中很多课程的讲解都是零散的理论知识介绍，时间跨度大，一个知识模块往往需要讲解半年或两三个月时间，前后知识不连贯，学习新知识时往往会忘记旧知识。而且很多课程的讲解不能够和现实网络环境相结合，即便是学习完知识，学生依然不知道如何使用这些技术。

结合以上问题，如何能让有意向成为网络工程师、网络管理员、网络安全工程师的人在负担较小经济压力的前提下学到有价值的东西，成为社会的需求。

而本书就是针对这一需求定制的。编者在网络工程、网络管理、网络安全方面从事了多年研究及毕业生培训、实训工作，本书集结了编者多年的研究成果和实践经验。

本书内容

本书主要介绍的是针对中小型企业的网络管理维护技术，并基于 Windows 的操作系统平台。本书理论联系实际，通过典型的实例向大家介绍网络管理的知识。

第 1 章主要介绍搭建企业网络环境的流程，包括需求分析、设计网络实施方案、设备选型和采购、地址规划、绘制网络拓扑图等；还介绍了维护企业网络环境的方法，以及网络管理实施方案的设计。

第 2 章主要介绍网络设备概述，网络设备的管理连接方法，构建路由交换模拟实验环境的方法，网络设备的加密、IOS 和配置文件的备份恢复、远程管理多台设备、快速配置多台设备的方法。

第 3 章介绍在网络中典型的路由交换技术配置案例，包括 VLAN 配置、STP 二层网络冗余配置、VRRP 三层网络冗余配置、端口捆绑、ACL 访问控制列表配置、QoS 服务质量配置、NAT 地址转换配置、VPN 虚拟专用网配置等。

第 4 章介绍企业无线局域网实施方案，包括需求分析、方案设计、AP 分布、无线设备配置等；还介绍了常见无线网络故障的诊断与排除方法。

第 5 章介绍单机故障的分类、故障原因分析方法、常见硬件故障分析解决方案、常见软件故障分析解决方案、BIOS 配置全攻略等内容。

第 6 章介绍企业服务器管理概述、服务器的选型与安装、服务器系统的操作基础、DHCP 服务器的搭建与管理、打印机服务器的搭建与管理等内容。

第 7 章介绍 FTP 服务器概述、常用的搭建 FTP 服务器的软件、高校 FTP 服务器案例分析、使用 Serv-U 软件搭建与管理 FTP 服务器的方法等内容。

第 8 章介绍企业邮件服务器概述、搭建邮件服务器前的准备工作、使用 U-Mail 邮件服务器程序的方法及安全管理。

第 9 章介绍企业网站管理概述、IIS 组件的安装、简单网站的发布、多网站发布方法、使用 CA 证书构建 SSL 安全发布 Web 环境。

第 10 章介绍常见的企业动态网站发布环境配置方法，包括 ASP.NET 动态网站发布、JSP 动态网站发布、PHP 动态网站发布等。

第 11 章介绍常用企业服务器对外发布的方法及操作环节。首先是域名的申请注册及管理，其次是虚拟空间或虚拟主机的选择与申请，最后是远程管理服务器空间。

第 12 章介绍网络存储服务器概述、RAID 磁盘容错技术的使用、磁盘配额的配置、数据备份计划的配置、磁盘阵列柜概述、存储磁盘损坏后的数据恢复等内容。

第 13 章介绍企业 OA 办公自动化系统的维护与管理，包括企业 OA 办公自动化系统概述、通达 OA 软件的安装与调试、员工权限管理、OA 账户管理、信息通信与共享管理、企业新闻和公告管理、企业工作流创建与使用等内容。

第 14 章介绍 Windows 群集的管理，包括 NLB 网络负载平衡群集的准备、配置和验证，故障转移群集的准备、安装、验证和建立群集。

第 15 章介绍网络数据库管理与维护概述，并以 MySQL 数据库为例介绍了数据库的安装、配置、启用、创建与删除、备份与还原、迁移等内容。

第 16 章介绍 SolarWinds 网络管理工具概述、SNMP 网络管理协议的配置、SolarWinds 网络管理工具的安装、常见工具组件 IP Network Browser 和 Network Performance Monitor 等的使用。

第 17 章介绍网络管理平台概述、主流网络管理平台、Spiceworks 网络管理平台的架设和应用、WhatsUp Gold 网络管理平台的架设和应用。

第 18 章介绍网络流量监测分析的意义、主流流量探测分析工具、利用镜像端口获取网络流量的环境部署、科来网络分析系统的安装和使用、Sniffer Pro 网络嗅探工具的安装与使用。

第 19 章介绍反病毒系统概述、企业反病毒系统的设计原则，以及 ESET NOD32 企业反病毒系统和趋势科技企业反病毒系统的安装、配置和使用。

第 20 章介绍企业防火墙概述、防火墙的分类、防火墙的联网模型、防火墙产品选购原则、带 DMZ 隔离区的 ISA 企业防火墙的架设方法、使用 ISA 防火墙控制员工的网络访问行为（上网时间、网站访问、网络下载）的配置、企业关键服务器的发布。

本书特色

- 理论联系实际：本书以简单理论概述引入知识，结合实际工程案例进行技术讲解与演示，可以帮助读者快速地掌握技术用途及实施方法。本书多采用中小型企业中使用较多，安全性、稳定性较高的软硬件产品工具。
- 一步一图，图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程及效果，便于更快地理解和掌握。
- 易学易用：颠覆传统“看”书的观念，变成一本能“操作”的图书。
- 实训效果：本书采用案例介绍、需求分析、实施流程规划、分步施工的顺序组织内容，方便读者系统地、模块化地学习，能够达到网络实习的效果。

读者对象

本书是一本完整介绍中小型企业网络管理的应用知识的教程，内容丰富、条理清晰、实用性强，适合以下读者学习使用：

- 对中小型企业网络管理感兴趣的零基础读者；

- 计算机网络技术、网络工程、网络安全相关专业的学生;
- 具有一定的网络基础知识，熟悉网络路由交换技术和网络服务器技术，能够实现简单网络搭建，对网络管理技术、网络安全技术感兴趣的工程师;
- 各行各业需要学习网络管理知识的人员。

鸣谢

本书作者长期从事网络实训的培训工作。参与本书的编写人员除了封面署名人员以外，还有刘玉萍、王英英、姬远鹏、王攀登、张工厂、王婷婷、苏士辉、肖品、张少军、孙若淞、宋冰冰、王维维、梁云亮、程铖、臧顺娟、陈伟光、卢健良和李亚飞等人。虽然倾注了编者的努力，但由于水平有限、时间仓促，书中难免有错漏之处，欢迎读者指正。如果遇到问题或有意见，敬请与我们联系，我们将全力提供帮助。

编　者

2012 年 3 月

目　　录

第 1 章　搭建与维护企业网络环境 1

1.1　搭建企业网络环境 1

1.1.1　网络环境需求分析 1

1.1.2　项目实战 1：设计合理的网络实施方案 2

1.1.3　设备选型和采购 5

1.1.4　项目实战 2：规划高效的网络地址 8

1.1.5　项目实战 3：绘制网络拓扑图 11

1.2　维护企业网络环境 16

1.2.1　规范网络管理的范围和任务 16

1.2.2　项目实战 4：获得网络基本信息 17

1.2.3　项目实战 5：设计网络管理实施方案 21

1.3　专家答疑 29

第 2 章　网络设备管理与维护基础 31

2.1　企业网络设备概述 31

2.2　项目实战 1：采用多种方法连接配置网络设备 32

2.2.1　Console 口直连配置 32

2.2.2　Telnet 远程登录配置 34

2.2.3　HTML 网页连接配置 36

2.3　构建路由交换模拟实验环境 36

2.3.1　安装 DynamipsGUI 模拟器 37

2.3.2　使用 DynamipsGUI 模拟器 39

2.4　网络设备常用配置案例 44

2.4.1　项目实战 2：备份与恢复设备配置文件 45

2.4.2　设备加密 48

2.4.3　项目实战 3：网络设备密码恢复 50

2.4.4　项目实战 4：设备 IOS 的备份、恢复和更新 51

2.4.5　项目实战 5：Telnet 远程管理多个设备 53

2.4.6　项目实战 6：使用脚本快速配置多台网络设备 56

2.4.7　设备连通测试命令——ping 57

2.5　专家答疑 58

第 3 章　常用网络工程配置实例 59

3.1　优化局域网环境 59
3.1.1　使用 VLAN 技术 59
3.1.2　使用 MAC 地址绑定技术 62
3.1.3　项目实战 1：使用 VTP 快速配置 VLAN 63
3.2　使用冗余技术提高网络可用性 66
3.2.1　运用 STP 提供二层链路冗余 66
3.2.2　使用 VRRP 提供三层网关冗余 67
3.2.3　项目实战 2：使用三层交换机实现基于 VLAN 的多层冗余 68
3.3　如何解决链路带宽不足 76
3.3.1　升级网络至千兆网络环境 76
3.3.2　增加链路数量 76
3.3.3　项目实战 3：使用以太网信道（端口聚合）增加主干链路带宽 77
3.4　网络流量控制 78
3.4.1　访问控制列表 78
3.4.2　服务质量 81
3.4.3　项目实战 4：使用扩展访问控制列表确保 VLAN 间安全访问 84
3.5　企业网络出口的 NAT+ACL 方案实现 86
3.5.1　NAT 地址转换技术概述 86
3.5.2　项目实战 5：为企业对外发布服务器配置静态 NAT 87
3.5.3　项目实战 6：为企业员工配置基于端口的动态地址转换技术 PAT 88
3.5.4　项目实战 7：实现出口 NAT 的双线接入 89
3.6　企业分支机构通信安全 92
3.6.1　VPN 技术介绍 92
3.6.2　IPSec VPN 配置原理 95
3.6.3　项目实战 8：使用 IPSec VPN 技术实现企业分支机构安全连接 96
3.7　专家答疑 99

第 4 章　企业无线网络管理与维护 100

4.1　无线局域网概述 100
4.2　无线网络方案实施 101
4.2.1　无线网络需求分析 101
4.2.2　无线网络方案设计 101
4.2.3　规划无线 AP 的分布 102
4.2.4　项目实战 1：配置无线路由器，并实现无线网络环境的安全加密 103
4.3　无线网络故障诊断与排除 117
4.3.1　项目实战 2：无线网络连接与通信故障 117
4.3.2　项目实战 3：无线网络共享与安全故障 118

4.3 专家答疑 119

第 5 章 单机故障检测分析 120

5.1 单机故障处理的基础 120
5.1.1 硬件故障 120
5.1.2 软件故障 120
5.2 单机故障产生的原因 121
5.3 故障诊断的原则和方法 123
5.3.1 单机故障诊断的原则 123
5.3.2 单机故障诊断的方法 124
5.4 常见硬件故障分析及解决方案 127
5.4. 1 常见 CPU 故障现象及解决方案 127
5.4.2 常见内存故障现象及解决方案 129
5.4.3 常见硬盘故障现象及解决方案 131
5.4.4 常见显卡故障及解决方案 134
5.4.5 计算机死机或重启故障分析及解决方案 136
5.5 常见软件故障分析及解决方案 138
5.5.1 系统蓝屏故障分析及解决方案 139
5.5.2 系统死机分析及解决方案 145
5.5.3 注册表常见故障分析及解决方案 147
5.5.4 键盘无法输入故障的解决方案 150
5.5.5 BIOS 密码忘记解决方案 150
5.6 项目实战：BIOS 设置全攻略 152
5.6.1 BIOS 介绍与常用设置 152
5.6.2 常见 BIOS 故障及其解决方案 157
5.7 专家答疑 157

第 6 章 企业服务器管理与维护 160

6.1 企业服务器管理概述 160
6.2 服务器的选型与安装 161
6.2.1 服务器的选型 161
6.2.2 服务器的压力测试 162
6.2.3 安装 Windows Server 2008 的准备工作 162
6.2.4 项目实战 1：安装 Windows Server 2008 操作系统 163
6.3 服务器系统操作基础 166
6.3.1 利用任务管理器查看系统运行状态 166
6.3.2 本地用户和组分配与权限管理 168
6.3.3 项目实战 2：配置组策略提高系统安全 172

6.3.4 项目实战 3：系统服务管理与系统瘦身 177
6.3.5 项目实战 4：利用系统开机启动项和进程发现计算机病毒和木马 178
6.4 DHCP 服务器的搭建与管理 180
6.4.1 架设 DHCP 服务器 180
6.4.2 作用域的分配与创建 186
6.4.3 为服务器配置保留地址 191
6.4.4 项目实战 5：备份与还原 DHCP 服务器的配置 192
6.4.5 项目实战 6：DHCP 服务器迁移 194
6.5 打印服务器搭建与管理 195
6.5.1 企业打印机的规划与采购 195
6.5.2 项目实战 7：安装企业打印机 196
6.5.3 项目实战 8：实现打印机全网共享使用 208
6.6 专家答疑 211

第 7 章 FTP 服务器搭建与维护 213

7.1 FTP 服务器概述 213
7.1.1 什么是 FTP 服务器 213
7.1.2 搭建 FTP 服务器的软件 213
7.1.3 高校 FTP 服务器案例分析 214
7.2 项目实战：使用 Serv-U 搭建企业文件服务器 215
7.2.1 安装 Serv-U 软件 215
7.2.2 为用户分配 FTP 账户及空间 217
7.2.3 实现同一账户在多网段访问具有不同权限 229
7.2.4 建立账户虚拟目录，实现多层次的账户目录管理 236
7.3 专家答疑 243

第 8 章 企业邮件服务器的搭建与维护 244

8.1 企业邮件服务器概述 244
8.1.1 企业邮件服务器介绍 244
8.1.2 搭建邮件服务器前的准备工作 244
8.2 项目实战：搭建 U-Mail 邮件服务器 246
8.2.1 邮件服务器方案介绍 246
8.2.2 安装配置 DNS 服务器 247
8.2.3 安装 U-Mail 邮件服务器 254
8.2.4 使用管理账户配置邮件服务器 257
8.2.5 为企业员工分配邮件账户 262
8.2.6 反垃圾邮件和个人邮箱限制 264
8.3 专家答疑 268

第 9 章　企业网站的搭建与维护 269

9.1　企业网站管理概述 269
9.1.1　IIS 介绍 269
9.1.2　搭建企业网站环境的准备工作 269
9.2　项目实战 1：搭建企业网站环境 269
9.2.1　安装 Web 服务器（IIS 组件） 270
9.2.2　发布网站 274
9.3　使用 IIS 进行多网站发布 277
9.3.1　使用不同的 IP 发布不同的网站 277
9.3.2　使用同一 IP 地址不同的端口发布不同的网站 282
9.3.3　利用不同主机头发布不同的网站 284
9.4　项目实战 2：使用 SSL 确保 Web 服务器通信安全 286
9.4.1　建立 CA 服务器 286
9.4.2　在 Web 服务器上制作证书申请文件并申请证书 295
9.4.3　CA 颁发证书 300
9.4.4　Web 服务器下载并安装证书 300
9.4.5　客户端信任 CA 安全访问网站 304
9.5　专家答疑 308

第 10 章　发布企业动态网站 309

10.1　发布 ASP.NET 动态网站 309
10.1.1　安装 IIS 组件支持 ASP.NET 309
10.1.2　网站发布 312
10.2　发布 JSP 动态网站 315
10.2.1　安装 JDK 并配置环境变量 315
10.2.2　安装 Tomcat 并配置环境变量 319
10.2.3　检测 Tomcat 平台 324
10.2.4　用 JK 整合 IIS 6 与 Tomcat 6 326
10.3　发布 PHP 动态网站 333
10.3.1　安装 MySQL 333
10.3.2　安装 PHP 339
10.3.3　IIS 与 PHP 的整合配置——发布 PHP 动态网站 340
10.4　专家答疑 344

第 11 章　企业服务器的对外发布与管理 345

11.1　域名注册 345
11.1.1　域名的选择 345

11.1.2 项目实战 1：注册域名 345
11.1.3 管理域名 352
11.2 虚拟空间申请 354
11.2.1 虚拟空间和虚拟主机的选择 354
11.2.2 申请虚拟主机 355
11.3 管理企业服务器 356
11.3.1 项目实战 2：使用远程桌面管理服务器 356
11.3.2 项目实战 3：使用 FTP 管理远程 Web 服务器 356
11.4 专家答疑 358

第 12 章 企业网络存储服务管理与维护 359

12.1 网络存储服务器概述 359
12.2 项目实战 1：磁盘管理基础配置 359
12.2.1 使用 RAID 磁盘容错技术配置分区 359
12.2.2 为账户设定磁盘配额 370
12.2.3 设定系统的数据备份计划 372
12.3 项目实战 2：使用磁盘阵列柜 381
12.3.1 认识磁盘阵列柜 381
12.3.2 存储磁盘损坏后的数据恢复 382
12.4 专家答疑 385

第 13 章 企业 OA 办公自动化系统的维护与管理 386

13.1 企业 OA 办公自动化系统概述 386
13.2 项目实战 1：搭建 OA 办公自动化环境 387
13.3 项目实战 2：配置管理 OA 系统，实现办公自动化 389
13.3.1 实现员工权限设置管理 390
13.3.2 实现 OA 账户管理 393
13.3.3 实现通信与信息共享 398
13.3.4 企业新闻和公告管理 401
13.3.5 实现企业信息自由交流 409
13.3.6 实现文件管理与共享 417
13.4 企业工作流的创建与使用 424
13.4.1 工作流概述 424
13.4.2 项目实战 3：创建企业出差请假工作流 424
13.4.3 项目实战 4：出差请假工作流的实际使用 441
13.5 专家答疑 446

第 14 章 Windows 群集的管理 447

14.1 Windows 群集概述 447
14.1.1 网络负载平衡群集 447
14.1.2 故障转移群集 448
14.2 项目实战 1：配置 NLB 群集 449
14.2.1 完成 NLB 群集的准备 449
14.2.2 配置 NLB 群集 450
14.2.3 验证 NLB 群集 457
14.3 项目实战 2：创建故障转移群集 458
14.3.1 完成故障转移群集的准备 458
14.3.2 配置域环境 458
14.3.3 安装故障转移群集 465
14.3.4 验证故障转移群集配置 467
14.3.5 建立群集 471
14.4 专家答疑 474

第 15 章 网络数据库管理与维护 475

15.1 常见数据库介绍 475
15.2 项目实战 1：MySQL 数据库安装与配置 476
15.2.1 在 Windows 平台下安装与配置 MySQL 476
15.2.2 配置 MySQL 5.5 480
15.3 项目实战 2：MySQL 数据库的启用与管理 485
15.3.1 启用 MySQL 485
15.3.2 数据库的创建与删除 489
15.4 项目实战 3：数据库的备份与恢复 493
15.4.1 数据备份 493
15.4.2 数据还原 497
15.4.3 数据库迁移 498
15.4.4 综合案例 500
15.5 专家答疑 503

第 16 章 SolarWinds 网管工具的使用 505

16.1 SolarWinds 工具介绍 505
16.1.1 SolarWinds 网管工具概述 505
16.1.2 项目实战 1：配置 SNMP 网络管理协议 506
16.2 安装 SolarWinds 网管工具 512
16.3 项目实战 2：使用 SolarWinds 网管工具 513

16.3.1　IP Network Browser 513
16.3.2　Network Performance Monitor 519
16.3.3　其他网络管理小工具 522
16.4　专家答疑 529

第 17 章　网络管理平台的架设与使用 530

17.1　网络管理平台介绍 530
17.1.1　什么是网络管理平台 530
17.1.2　主流网络管理平台产品 533
17.2　项目实战 1：搭建 Spiceworks 网络管理平台 535
17.2.1　网络管理环境搭建 535
17.2.2　架设网络管理平台 536
17.2.3　应用网管平台 544
17.3　项目实战 2：搭建 WhatsUp Gold 网络管理平台 550
17.3.1　架设网络管理平台 550
17.3.2　实现网络环境监控 553
17.3.3　查看网络设备信息 559
17.3.4　网络故障发现与修复 561
17.4　专家答疑 564

第 18 章　网络流量监测分析 565

18.1　网络流量分析的意义 565
18.2　主流产品技术分析 565
18.2.1　Sniffer Pro 网络嗅探工具概述 566
18.2.2　科来网络分析系统 567
18.3　科来网络分析系统的安装与使用 568
18.3.1　安装科来网络分析系统 568
18.3.2　设置过滤器 571
18.3.3　使用科来网络分析系统分析 ARP 异常 573
18.4　项目实战：使用 Sniffer Pro 进行网络流量监控分析 575
18.4.1　安装 Sniffer Pro 网络嗅探工具 576
18.4.2　设置 Sniffer Pro 监控网络适配器 580
18.4.3　Sniffer 的监控功能 581
18.4.4　捕捉数据包 588
18.4.5　分析造成网络速度慢的原因 597
18.4.6　查找网络 ARP 攻击源 598
18.5　专家答疑 601

第 19 章　企业网络病毒防护系统架设与使用 603

19.1　反病毒系统概述 603
19.1.1　企业反病毒的定义 603
19.1.2　企业反病毒系统的设计原则 603
19.2　项目实战 1：ESET NOD32 企业反病毒系统实战案例 604
19.2.1　安装 ESET NOD32 企业反病毒系统 604
19.2.2　设置 ESET 配置编辑器 610
19.2.3　设置客户端连接 618
19.2.4　使用 ESET NOD32 进行全网杀毒 621
19.3　项目实战 2：趋势科技企业反病毒系统实战案例 622
19.3.1　安装趋势科技企业反病毒系统 622
19.3.2　设置趋势科技软件防护内网安全 628
19.3.3　使用趋势科技软件进行全网杀毒 638
19.4　专家答疑 640

第 20 章　企业防火墙架设与使用 641

20.1　防火墙概述 641
20.1.1　企业防火墙 641
20.1.2　防火墙的分类 642
20.1.3　防火墙联网模型 643
20.1.4　产品选型 645
20.2　项目实战 1：架设 ISA 企业防火墙 646
20.2.1　模拟企业网络搭建实验环境 646
20.2.2　安装 ISA Server 2006 防火墙 647
20.2.3　添加 DMZ 区，改变 ISA 联网模式 651
20.3　项目实战 2：利用 ISA 控制员工上网 655
20.3.1　允许员工访问互联网 656
20.3.2　限制员工的上网时间 659
20.3.3　限制员工访问特殊域名网站 661
20.3.4　限制员工使用迅雷等下载工具 663
20.4　项目实战 3：利用 ISA 发布企业内网服务器 667
20.4.1　ISA 防火墙安全发布 Web 服务器 667
20.4.2　ISA 防火墙安全发布邮件服务器 672
20.4.3　ISA 防火墙安全发布其他服务器 674
20.5　专家答疑 677

第 1 章　搭建与维护企业网络环境

随着网络技术的发展，网络应用已深入人们生活中的各个方面。越来越多的企事业单位开始建立或者已经建立了自己的网络办公环境，以实现高效的网络办公和内部管理。因此，懂得如何建立一套良好的企业网络环境，以及如何对一个现有的企业网络环境进行维护，就成了一门必修课。本章将系统介绍如何搭建、维护企业网络。

1.1　搭建企业网络环境

企业网络环境建设是一个从无到有的过程。在整个过程中会有很多因素和细节需要解决和考虑，涉及对所有网络技术的综合应用。具体到流程方面主要包括：需求分析、方案设计、设备选择、地址规划、拓扑设计等几个重要环节。下面将对其分别进行介绍。

1.1.1　网络环境需求分析

网络环境需求分析是在开始建立网络系统之前，对用户办公环境所做的一次详细的调查和记录工作。在调查中需要与用户进行直接沟通交流和实地考察，了解用户对整个网络功能特性的要求，从而实现网络系统建设的实用性和远期目标性。

具体操作事项可依据如下内容进行。

1. 用户目标调查

调查了解用户目标，明确本次工程属于新的建设还是原有改造。然后，依据工期制定出明确的近期工程目标，即网络系统建成以后短期内需要达到的一个功能和效果。另外，就是远期目标，主要体现网络系统在将来可具有的一个扩展空间和升级能力，实现网络系统的最高性价比。

2. 网络系统物理布局

对于网络系统物理布局，主要了解用户建筑布局、建筑结构和用户信息点数量，如果是改造工程还包括目前网络环境、设备位置、设备数量、互连状况、IP 信息等情况。这些情况都是网络工程布线系统的基本信息，同时也都是进行 VLAN 划分或者子网规划的一项重要依据。

3. 网络性能需求

网络性能需求包括用户对网络延时、带宽、可靠性、服务质量等方面的要求。而这些方面的需求程度，直接决定着网络系统的规模和难度以及需要的资金投入，同时也是设备选取时所要考虑

的首要因素。获取的方式可采用将专业的技术转化为基本的问题进行。最后，进行整理并做出相应的分析和判断。

4. 网络服务需求

对于服务需求，主要是调查用户对网络应用方面的要求。例如：用户是否需要 Web 应用、FTP 应用、数据库系统应用和 OA 系统应用。一般情况下，在网络系统中都会部署相应的应用服务器，以提供日常业务应用服务，但这种需求随着不同的用户会有很大的差异。因此，作为网络系统部署中服务应用实施的重要参考，必须要做到有针对性的调查和了解。

5. 网络系统安全性需求

对于安全性需求，可从数据存储、数据传输和服务应用三个层次进行调查了解。现实中网络技术的快速发展，虽然产生了很多新的应用，但也因此带来了更多的安全性威胁。因此，对于网络安全性的防护也成了用户关注的一个重点，也自然是调查了解的重点。另外，通过对网络安全性需求的了解，也可以明确用户对网络环境的重视程度和应用深度，对网络方案的整体设计是很重要的参考资料。

总之，网络需求了解要做到尽可能细致、广泛和全面。从而，使后期的方案设计和实施可以有更为充分的依据。

1.1.2 项目实战 1：设计合理的网络实施方案

本节以一个中小型企业网络建设项目为案例，简要说明在实际场景中应如何进行网络前期的需求了解、分析，并最终形成可行的网络实施方案的过程。

1. 项目介绍

这是一家制造型企业，成立于 2006 年，主要经营业务为玻璃制品生产。历经 5 年的发展，企业已初具规模，并新建了办公用房和厂房。因此，为进一步加强企业管理、提高生产效率、加快企业发展，企业决定重新部署和建设一套自己的网络办公应用系统。

2. 用户需求分析

1）用户目标情况

经过与用户企业的沟通交流，本次工程建设属于厂区在原有设备上的重新搭建。基本目标是满足一体化的快捷办公需求，改变原有分散办公不易管理的情况。同时，新建成的网络系统要能适应 5 年以内的应用变化情况。

技术分析：从目标来看，需要重点关注智能办公系统建设，网络基础设备要采用技术实力较好的品牌，如华为、中兴、H3C 等厂家产品。另外，原有设备在可用的情况下做好重复再利用以节约项目投资。

2）网络物理系统布局情况

经过实地考察了解到，企业目前有自己的网络机房但线路杂乱，整个网络为交换设备通过路由接入到互联网的简单模式。在沟通中，用户表示网络经常因网络设备故障引起通信中断。而当信

息点出现问题时，故障检测很困难。后期，依据实际考察的情况，对相应的设备位置、数量、信息点接入数量以及原有建筑结构和新建筑结构情况进行统计汇总，并以表格的形式呈现。下面给出相应的参考样表，分别如表 1-1 和表 1-2 所示。

表 1-1 建筑结构情况记录

建筑名称	建筑层数	建筑层高	层内办公室分布	信息点数

表 1-2 目前设备信息

设备名称	设备数量	设备位置	设备状态	业务应用	IP 信息

3）网络性能需求

在交流过程中，用户要求新的网络系统一定要保证快速的反应能力，解决原来网页打开缓慢、下载缓慢以及内部服务器无法访问的问题。同时，新的网络系统一定要可靠，防止因一条线路故障或者一台设备故障导致全网中断的情况发生。

技术分析：要解决这一需求，方案中要考虑使用双线冗余、外网出口双线负载以及流量控制机制的形式。同时，通过科来、Sniffer 等工具设立专用的网络平台，实时监控网络的运行状态。

4）网络服务需求

在用户环境中，用户目前除财务系统以外，暂无其他网络服务应用。于是，在新的网络系统工程中，客户要求能够实现在线办公交流的应用、有企业自己的邮箱收发往来的业务邮件、有可以对外宣传企业的网站服务、有管理仓库进出情况的应用以及可以从内部分享资源的应用。

技术分析：依据企业用户提议需要在方案中合理部署财务系统应用、OA 系统应用、Web 系统应用、E-mail 系统应用、ERP 仓库系统应用以及 FTP 文档服务应用。

5）网络系统安全性需求

对于安全性方面，通过对用户的引导，用户反映有很多安全方面的问题需要解决。首先，很多员工不知怎样合理安装和使用杀毒软件，经常出现因病毒导致的计算机问题。其次，公司数据库系统总是受到外部网络的威胁，使得公司整个财务系统不得不与整个外网和内部其他网络分离，给工作上带来了很大的影响。最后，就是内部用户之间的访问控制，在原有的网络环境下总是不能得到很好的控制。

技术分析：对于这一需求，结合用户实际情况，安装专业的网络反病毒防护系统和安装隔离

策略，如江民网络版、SAV 网络版等产品。

3. 具体实施方案设计

（1）选择使用华为品牌设备，以实现良好的可管理功能和后期扩展功能，并可获得后期良好的技术支持服务。

（2）网络设备互连架构设计，依然采用核心层、汇聚层、接入层三层模式建立。

- 核心层提供全 1000M 服务应用，为全网提供应用服务器数据访问工作。同时，也负责全网的安全数据防护和互联网访问流量控制管理功能。
  设备采用可插卡扩容的产品型号，并采用两台互为冗余备份的核心交换设备、一台服务器和互联网接入专用交换设备的架构模式。
  设备间连接使用高质量的六类双绞线缆，实现全 1000M 互连时高数据传输的需求。
  互联网接入使用双路光纤模式，并采用负载平衡技术，以实现高带宽互联网应用，并且在互联网接口处部署安全防火墙设备实现外网访问的高效防护。
  互联网接入路由设备部署 P2P 流量限定功能，以防止内部用户 P2P 下载对网络性能产生的影响。
  不同应用之间采用 VLAN 的形式实现隔离和策略控制，最后整理每条线路并加贴标签。
- 经过物理环境调查表格分析，汇聚层线路将采用双路 1000M 光纤的形式接入机房核心交换设备。
  对调查表中信息点密集的地址进行 VLAN 划分和子网规划，实现网络的高可用性。同时，安排放置具有三层交换功能的汇聚设备，为 VLAN 提供网关功能并实施相应的安全控制策略。
- 接入层采用二层交换设备，并依据办公室或者建筑楼层划分相应的子网和 VLAN，同时通过三层汇聚设备实现 VLAN 间的互通和控制。
  接入交换设备采用 100M/1000M 双路六类双绞线缆的形式与汇聚设备进行互连，以实现高可靠性和冗余。

最后，依据各实际位置信息点数调查情况，确定网络设备在相应的信息点区所应提供的接口数量，并统计成表格的形式留存。

（3）网络服务设备部署设计：

- 网络服务部署设施在机房中，并通过 1000M 接口与核心交换设备互连互通。
- 服务器架构总体设计依据前台显示和后台处理分离的模式，将财务系统和仓库管理系统所用的后台数据库系统和前台用户接口部署到相应的服务器设备中，以实现安全性和快速响应能力。
- 其他服务器应用采用应用整合的形式，这样一方面可以方便管理，另一方面可以节约投资。具体将 E-mail 和 Web 应用进行整合，将 OA 系统和 FTP 文档系统进行整合。
- 部署实施专用的数据备份服务设备，为所有服务应用中的重要数据提供备份存储功能。
- 为每项服务应用划分各自独立的子网空间并通过 VLAN 应用实现彼此业务隔离，以保证应用数据间的安全性。

（4）布线系统设计：

- 机房布线采用地面布放的形式，机房中安装相应的防静电地板，之后将线路整齐布放到地板下。
- 建筑楼内，采用水平天花板内捆扎布线和室内线槽布线的形式，并最后汇集到楼层交换设备间实现捆扎接入。
- 机柜内线路布置使用专门配线架和理线架，实现线路模块接入和标准捆扎。最后，对线路进行集中标签标识，做到美观整洁。以方便后期用户管理和维护。

1.1.3　设备选型和采购

在网络系统建设过程中，设备的质量、性能、功能等因素直接与网络系统的整体性能相关。而高质量的设备意味着更强的稳定性、更有利的网络性能和更出色的数据处理功能。但这样的设备在价格上，往往会超出一般企业用户所能承受的范围。因此，设备选择过程中要充分考虑两者的平衡点，这也是总的原则和方向。实施过程中，可具体从以下方面来作选择。

1. 设备的品牌选择

在网络系统设备市场中不同品牌的产品之间，在价格、性能、质量以及可管理性、安全性等方面都存在一定的差异。直观来讲，品牌决定了层次，而不同的层次也就意味这个厂商产品的整体档次。例如：选择在全球市场占有绝对优势的 Cisco 产品，与国内或国际其他产品相比，也就意味着选择了一个高层次、高质量。而在整个系统工程建设上也意味着更大的投入。所以，设备选型的首要任务就是要确定工程建设中各类型产品的品牌，明晰网络系统建设层次。那么，在实施过程中又应当如何确定使用哪种品牌呢？最简单的方式，依然是采用表格的对照方式来实现。而对于用户来讲，也会得到一个更为直观的感觉。表 1-3 给出了相应的参考样表。

表 1-3　设备品牌对照表

设备类型	品牌名称	产品种类	技术服务水平	平均故障率	平均使用寿命	市场占有率	市场价格水平

表 1-3 中各选项介绍如下。

- 设备类型：指在网络系统建设中需要购买实施的设备，如路由器、防火墙、交换机、服务器等设备。
- 品牌名称：这里写入可供参考的设备的品牌名称。
- 产品种类：写明一个品牌下所能提供的相关产品，与设备类型形成对应关系。例如：Cisco 就可以提供路由器、交换机、防火墙等网络产品设备。
- 技术服务水平：写入某一品牌的市场评价、技术响应能力、问题解决能力、服务质量等因素的综合评定，可使用百分比或中、低、高档次进行表示。
- 平均故障率、平均使用寿命、市场占有率、市场价格水平：这些主要是展现不同品牌中同

一种类产品之间的性价比。内容信息可以通过市场调查、询问或互联网查询的方式获取。

通过对上述表格中内容的分析和对比，完全可以从整体上确定不同设备类型的相应厂商品牌。但在同一设备类型中，最后确定的品牌种类不得超过 2 种，以方便管理和保持良好的兼容性。

2. 设备的具体型号选择

确定设备品牌以后，设备的具体型号选择就是另一个需要重点关注的内容了。就如同写作一样，文章的文体确定完成以后，具体的内容组织结构也是决定整个文章质量的关键点。设备型号的选择也是如此，每一种品牌的产品都会有着很多的系列可供选择。例如交换机，在选定的任意品牌中，会包括三层设备型号、二层设备型号、光端口型号、电端口型号甚至直流供电和交流供电型号。而一个品牌中的服务器设备也同样存在很多子型号，每一个子型号之间也都有各自的差异性。例如 IBM System x3650 M3(7945O45)和 IBM System x3650 M3(7945I01)，从品牌来讲都是 IBM，只是 M3(7945O45)和 M3(7945I01)有所不同。但就这里的不同导致这两台设备在价格和性能上都产生了不小的差异。因此，在选择品牌以后，对品牌内部型号也要进行更为详细的对比和衡量。下面也列举一下相关的对比参考表格，分别如表 1-4~表 1-6 所示。

表 1-4　设备型号对照表——网络交换设备

品牌	型号	最大端口数	端口转发速率	最高包转发率	最高背板容量	市场价格	可否支持安全限定功能

表 1-4 中各选项介绍如下。

- 最大端口数：指交换设备所能承载的最大接口数量，由于交换设备有些是可自由选择的模块设备，因此在这里表示为“最大端口数”。而在每一款交换设备中，都会有很多种不同的端口数型号可供选择。例如，Quidway S2700 系列就可分为 2709、2718、2726、2752，分别为 9 端口、18 端口、26 端口、52 端口。但最后选择哪一端口数的设备主要依据需求分析中信息点数的详细记录进行选取。
- 端口转发速率、最高包转发率、最高背板容量：这是衡量一台交换设备性能的最主要指标。考虑到模块化交换设备，这里依然使用“最高”表示方式。“端口转发速率”表示设备接口为 100M、1000M 还是 10G。“背板容量”和 “包转发率”就分别好比一条高速公路的宽度和最高限定时速。而这些参数一般会随着不同的设备端口数而有不同的取值。
- 可否支持安全限定功能：主要考虑到网络系统中对子网之间数据防护的需要而参考的指标，包括设备是否支持 QoS、Traffic 策略限定、MAC 地址管制等功能特性。

表 1-5　设备型号对照表——网络路由设备

品牌	型号	最大端口数	端口转发速率	包转发率	数据吞吐率	并发连接数	参考价格	可否支持 P2P 限定功能

表 1-5 中各选项介绍如下。

- 型号：网络路由设备与交换设备一样，也存在很多不同的型号和类别。通常情况下，设备厂商会划分大的类型，之后再依据设备端口数、可活动插卡以及设备配置的不同划分小的型号。另外，随着产品的改进，防火墙这一类型的设备也可以实现路由器的功能，作为互联网出口接入设备。因此，这里的路由器也包含防火墙产品类型。而具体型号划分与传统的路由设备也大体相同。例如：Huawei Symantec 生产的 USG5120、USG5150 防火墙设备，其中 USG5100 为系列，20、50 为具体的小型号。它们在设备配置、活动插卡及接口上都有不同的差异。所以，在进行型号对比时一定要注意系列和型号的区别。
- 最大端口数：对于防火墙和路由器来讲，在内容上会有一定的差异。虽然，防火墙在技术上可以与路由器抗衡，甚至说在安全防护上优于路由器，而这也正是很多用户企业组建网络系统时选择它的缘由。但是路由器在对广域网接口类型和广域网协议的支持上要明显优于防火墙设备。因此，在网络系统建设过程中要充分考虑这些方面的因素。例如：网络系统中互联网接入设备采用的为以太网类型端口，那么在设备对比过程中写入的参考端口数量也就是以太网接口类型了。
- 端口转发速率、数据吞吐率、并发连接数、包转发率：这些为防火墙和路由器的主要性能指标，端口转发速率也指 100M 或 1000M 接口，数据吞吐率、并发连接数和包转发率分别表示设备在单位时间内所能承载的最大数据量和所能存储记录的最多数据连接信息。作为重点内容在进行对比时需要着重注意。
- 可否支持 P2P 限定功能：目前，在一些多功能路由器或者防火墙设备中，都支持 P2P 限定的功能。通俗来讲 P2P 就是数据的高速下载，也是很多情况下吃掉大部分出口带宽的主要因素。因此，很多企业用户都要求在网络建设过程中要在出口设备处部署 P2P 限定功能。在设备选择中也就需要关注这一功能的实现。

在表 1-6 中，每个条目内容都是经常听说过或见到过的参数指标。因此，具体的含义也就不再过多讲述。进行对照时要清晰辨别产品的型号，注意具体型号和系列的区别。同时，也要注意对比的对象之间要处于相同或相近的层级。例如，将 IBM 的一款高档服务器和 Dell 的中档服务器作对比，就是不合理的选择。

表 1-6 设备型号对照表——应用服务器设备

服务应用	品牌	产品型号	CPU 型号	最大 CPU 数	标配内存	最大内存容量	标配硬盘容量	最大硬盘容量	市场参考价格

不同的服务应用需要考虑不同层次的服务器系列和具体型号。因此，在选取时要做好服务应用的不同区分。基本方式可依据服务应用的重要性、用户访问量、数据存储容量等方面进行。

3. 设备采购

确定了设备的具体型号和参考价格，就可开始设备采购工作了。在设备采购过程中需要注意以下几点：

（1）要严格依据“网络系统物理布局”调查中确定的信息点数情况，和前期方案设计过程中确定的各不同区域所需的设备数量进行采购。总体原则：设备所支持的信息点数一定要大于或等于实际需求数量。

（2）设备购买是通过中间代理商，那么要查看代理商的资质信息，以防止采购的设备因渠道问题而无法得到后期技术支持。

（3）提交设备费用申请，申请获批以后，进行设备订购清单下发。在设备采购前一定要事先做好费用申请工作，对有疑问的地方及时处理和解决。

（4）设备运到后，要依据设备清单进行一一验收，并注意设备的安装配件是否齐全。防止后期因安装配件问题带来施工的困难。

1.1.4 项目实战 2：规划高效的网络地址

在网络领域中网络地址的规划和设计也是一门必修的基础课程。无论是在网络系统的建设中，还是在网络系统的管理中，网络地址都是受关注的问题，如地址类别选择、地址段选择、子网选择等。下面简单地向大家讲述地址的规划选择方法。

1. 网络地址基本情况

网络地址是TCP/IP这个协议家族中的一个重要成员，担负着网络层的数据标示工作。从TCP/IP网络层次模型来讲它处于第二网络接口层位置。而IP地址就是这里标示使用的数字。关于IP地址的基本信息如下：

（1）至目前为止，IP地址有IPv4和IPv6两种协议种类。虽然IPv6是未来的主导，但当前IPv4依然是主流应用。因此，下面内容涉及的IP地址统一为IPv4协议形式。

（2）IP地址表现形式为点分十进制形式，共分为4个8位二进制组，依据二进制到十进制转换法则，一个8位二进制组最大可转换到一个十进制的3位数。因此写法可表示为***.***.***.***。

（3）IP地址的类别分为A、B、C、D、E 5种。其中，A类、B类、C类、D类为可应用于网络产品中的类别。而A类、B类、C类为网络用户系统可自由使用的地址类别，D类为网络设备的特别功能使用。因此，在这里主要说明A类、B类、C类地址情况。另外，为区别各类地址，国际组织设定了相应的地址范围。

A类：1.0.0.1~126.255.255.254

B类：128.0.0.1~191.255.255.254

C类：192.0.0.1~223.255.255.254

地址中所显示的数字，都为二进制转换后的十进制数，即日常生活中所看到的形式。那么二进制如何转换为十进制？例如：********是8位二进制，上面可以写入的数字就是0或1两种。如果上面全部写入0，最后的十进制结果就是$0^7+0^6+0^5+0^4+0^3+0^2+0^1+0^0$；如果上面全部都写入1，最后的十进制结果就是$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$。其中的规律为$A^{n-1}$累加，当二进制位为0时A取0，

当二进制位为 1 时 A 取 2；n 为从右向左数时当前二进制位所在的位置。例如，第 1 个就是 1-1，第 2 个就是 2-1，第 3 个就是 3-1，依次类推。最后，将所有的值求和就是十进制数值。表 1-7 所示为 2 的幂次方对照表。

表 1-7　2 的幂次方对照表

2 的幂次方	值	2 的幂次方	值
2^{10}	1024	2^5	32
2^9	512	2^4	16
2^8	256	2^3	8
2^7	128	2^2	4
2^6	64		

1）IP 私网地址和 IP 公网地址

在 IP 地址应用过程中，为了区别普通用户网络系统和网络供应商用户网络系统，在不同的 IP 类别中划分出了两者各自使用的地址区间。而在企业用户网络系统建设中的地址规划，IP 私网地址才是真正的主角。各常用类别的私网地址范围为：

A 类：10.0.0.0~10.255.255.255　　默认掩码：255.0.0.0
B 类：172.16.0.0~172.31.255.255　　默认掩码：255.255.0.0
C 类：192.168.0.0~192.168.255.255　　默认掩码：255.255.255.0

2）地址子网和掩码

我国存在省、市、县三级行政机构。这使整个国家管理变得清晰、明了、有序。于是，在 IP 地址中也引入这样的层次结构，使网络系统的网络更为有效、合理、清晰。

首先，掩码也是一个 32 位的二进制位，表示方式与 IP 地址相同，即点分十进制。但它的比特位何时取 1、何时取 0 呢？例如：一个 172.16.0.0 掩码为 255.255.0.0 网络段，要求划分出 16 个子网段。其中，172.16 就是省名，而它对应的掩码之所以是 255.255.0.0，是因为 IP 技术规定，省名所在的二进制位置对应的掩码二进制位都必须写成 1，其他写成 0。因此，掩码的前两个 8 位组二进制位都变成了 1，后两个 8 位组二进制位都变成了 0。转化成十进制也就是 255.255.0.0。

现在要得到 16 个子网，也就是市名。依据常理，给市命名，省的名称一定不会改变的。最后一定是***省***市。那么，子网网号划分也是一样，172.16 就是固定的。因此，就只能从后面的那个 8 位组里拿出几位来做子网标记了。那么，该取几位呢？工程要求划出 16 个子网，也就需要 16 个不同的子网标记。假设现在面前有一堆牌，每张牌正反两面分别写有 0、1 两个数字。要求从中取出最少的牌，并能摆出形成 16 种不同的组合来。应该选择几张呢？结果应该是 4 张。因此，2^4=16。那么现在有 16 个子网等待着获得名称，应该选几个位呢？结果也是 4 位。之后，这 4 位的每一次不同的组合都将是一个不同的子网编号。表示为十进制：最小不会小于 0，最大不会大于 255。

到此为止，子网号确定了，那么掩码是多少呢？还是 255.255.0.0 吗？答案当然是否定的，因为，255.255.0.0 是省对于市来讲的“备案信息”。而市对于县来讲应该是另外的“备案信息”。与“省”规则一样，所有标识“市”的二进制位，在掩码中的对应位置也全部为 1。因此，子网的对应掩码自然就是 255.255.240.0。那么，除了“市”、“省”标号位以外的二进制位做什么用处呢？它们的功能就是标识“居民”门牌。也就是 IP 地址中的主机号，即用来标识用户计算机的地址位了。

2. 地址规划案例

现在依据案例再具体说明一次地址规划的操作手法：

（1）取出前期信息点调查信息汇总单，明确每个区域中的信息点的分布情况。

现有一栋办公楼共计 8 层，每层计算机数不大于 30 台，要求以每层为一个子网进行划分。

（2）选择 IP 类别。

A 类：默认掩码为 255.0.0.0。这意味着 IP 地址中第一个 8 位组为父网号，后面的 3 个 8 位组为可供用户自由使用的比特位，可以形成 2^{24} 种组合。其中，二进制位全为 0 的组合和全为 1 的组合不能使用，这也是国际规定的原则。而 2^3=8 从这里选取 3 位即可满足 8 个子网标识需求，同时后 3 个 8 位组还剩余 21 位，组合为 2^{21} 种减去 2 种规定不可使用的以后，剩余的数量远远大于 30 台主机 IP 的需求。因此，不符合 IP 地址尽可能节约使用的规则而放弃使用。

B 类：默认有 20 个主机位，取主机位的前三位做子网位可以获得 8 个子网，这样每个子网中拥有的主机位变成 17 位，那么一个子网中可容纳的主机数为 2^{17}-2，超出了每层不大于 30 台的限制，浪费地址，不符合规则。

C 类：掩码为 255.255.255.0。这意味着剩余一个 8 位组可以供划分子网号和主机号使用。取出 3 位做子网号，剩余 5 位，2^5 种组合，减去 2 种后，恰好可以满足 3 台计算机的标识。

（3）确定具体子网号和掩码。

第 1 个：192.168.0.0　　掩码：255.255.255.224
二进制为：11000000.10101000. 00000000. 00000000
　　　　　11111111.11111111.11111111.11100000
第 2 个：192.168.0.32　　掩码：255.255.255.224
二进制为：11000000.10101000. 00000000. 00100000
　　　　　11111111.11111111.11111111.11100000
第 3 个：192.168.0.64　　掩码：255.255.255.224
二进制为：11000000.10101000. 00000000. 01000000
　　　　　11111111.11111111.11111111.11100000
第 4 个：192.168.0.96　　掩码：255.255.255.224
二进制为：11000000.10101000. 00000000. 01100000
　　　　　11111111.11111111.11111111.11100000
……
第 8 个：192.168.0.224　　掩码：255.255.255.224
二进制为：11000000.10101000. 00000000. 11100000
　　　　　11111111.11111111.11111111.11100000

上面有阴影的比特位，分别为每个子网中主机的标识位。而当它们全部为 1 时，就是这个子网对应的广播地址；全为 0 时，则是本子网的子网号。这也就是在上文中计算子网内有效主机位组合的基础上减去 2 位的原因。

1.1.5 项目实战 3：绘制网络拓扑图

网络拓扑图是网络系统工程建设的图纸，是对工程实施方案的具体图形化描述。网络拓扑图一旦形成，就需要严格依据图中内容进行施工，不得随意修改。网络拓扑图的绘制方式很多，同时，也有很多工具可供选择。而在此主要介绍一款经典的绘图工具——Microsoft Office Visio 的使用方法。从名称中就可以得知，这是一款微软公司的产品，同时也是 Office 办公软件家族中的一个成员。目前，版本也已随着 Office 2010 的发布，有了最新 2010 版样式，但是在市场上主流实用的还是 2003 和 2007 两个版本。

在讲述如何通过它设计拓扑图之前，要先说明一下拓扑图绘制时应包含的基本要素。

1. 网络设备

网络设备是整张图中的点，将这些点连起来就形成了一个网、一个面。这些设备点包括：所有的网络数据传输设备（如路由器、交换机）和网络应用服务器设备（如网站服务器、文件服务器、数据库服务器等）。因此，拓扑中的设备要做到全面、准确、合理，不多余、不缺失。

2. 网络线路

网络线路就是实现图中点之间的连接。与综合布线图中的线路描绘不同的是，网络拓扑图中只会反映设备间的连接形式，绘制的所有线路要如实体现设备间的互连，做到细致、准确。不同的线路种类要通过不同的颜色、大小等进行突出标识。

3. IP 地址信息

IP 地址信息是另一个应当主要体现的信息，因为它们一般是不会在网络综合布线图中出现的，所以需要在网络拓扑中具体详细体现，进行相应的标注和标识，以保证网络工程建设的实际运作。

下面详细介绍使用 Office Visio 2003 绘制网络拓扑图的操作方法。

01 下载安装 Office Visio 2003，安装过程类似于其他 Office 办公软件。完成以后，选择【开始】➢【所有程序】➢【Microsoft Office】➢【Microsoft Office Visio 2003】菜单选项，如图 1-1 所示。

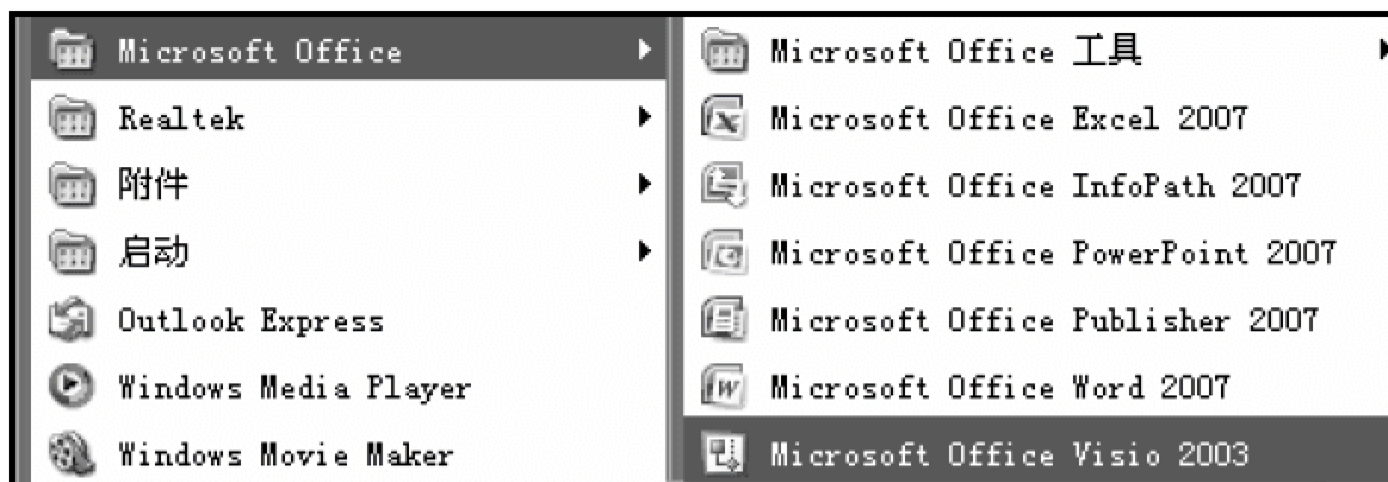


图 1-1　选择 Office Visio 程序

02 打开 Microsoft Office Visio 2003 程序主界面视图。在左侧的【类别】选项列表选择要绘制的图形类别。选择【网络】选项，并在右侧模板窗格中单击【详细网络图】图标，如图 1-2 所示。



图 1-2 选择 Visio 绘图类型

03 创建一个详细网络图的绘图，默认命名为“绘图 1”。图 1-3 所示为 Visio 程序主界面的介绍，该界面和 Office 办公软件家族中的其他程序界面相似。



图 1-3 Visio 程序主界面

04 从左侧的物体图标栏和已找好的图标库文件中选择需要的图标，并将其拖入或复制到工作区中，如图 1-4 所示。

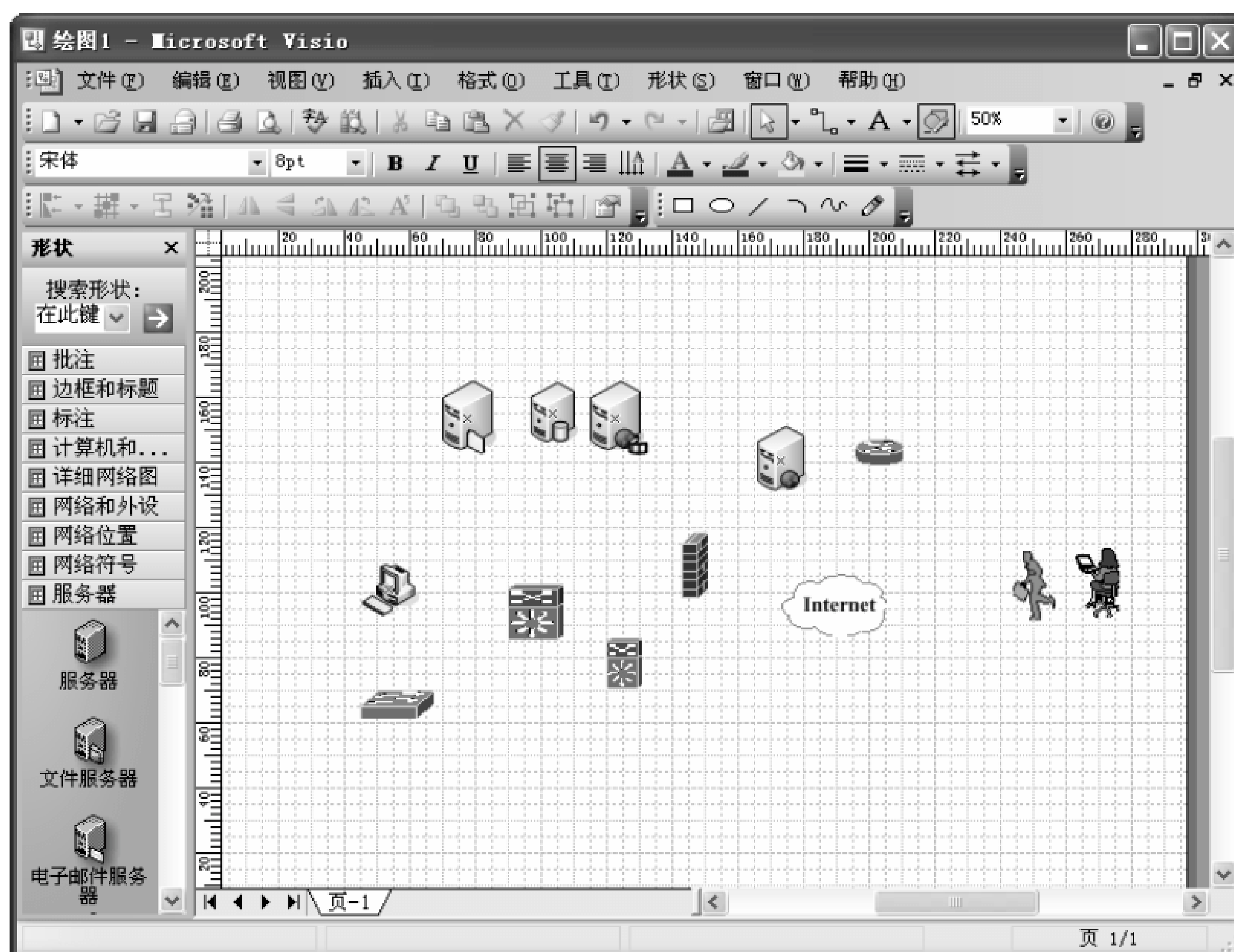


图 1-4　添加设备图标

05 根据设计的网络拓扑图需求，复制重复出现的图标，操作方法类似于通用 Office 办公软件，然后选中图标，使用鼠标拖动图标四周的顶点对其进行缩放操作，并使用移动工具将图标移至合适的位置，如图 1-5 所示。

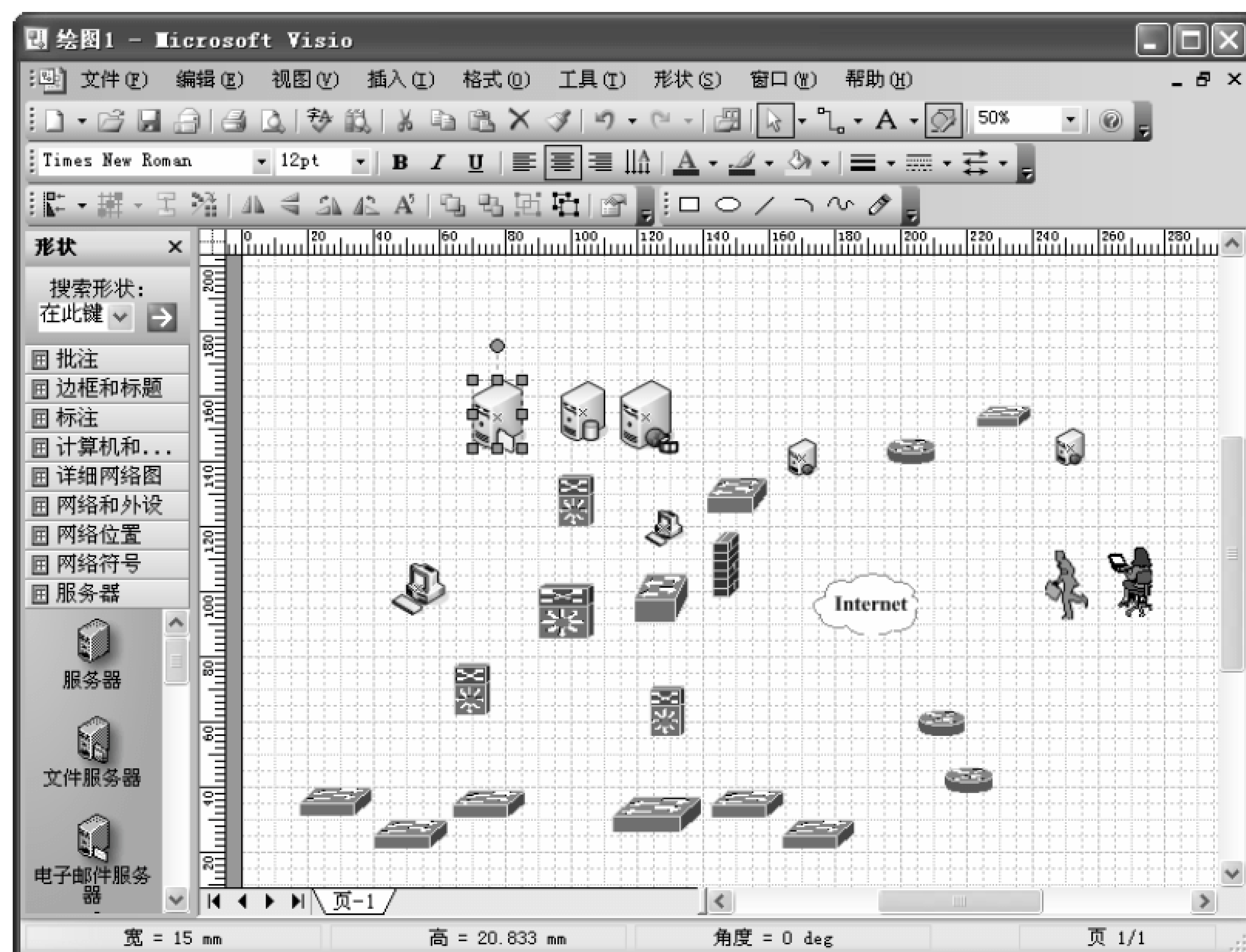


图 1-5　复制重复设备图标

06 位置、大小基本调整好之后，为了使拓扑图显得更加整齐，可以使用工具栏中的【对齐形状】和【分配形状】工具调整设备图标的水平位置及间距，如图 1-6 所示。

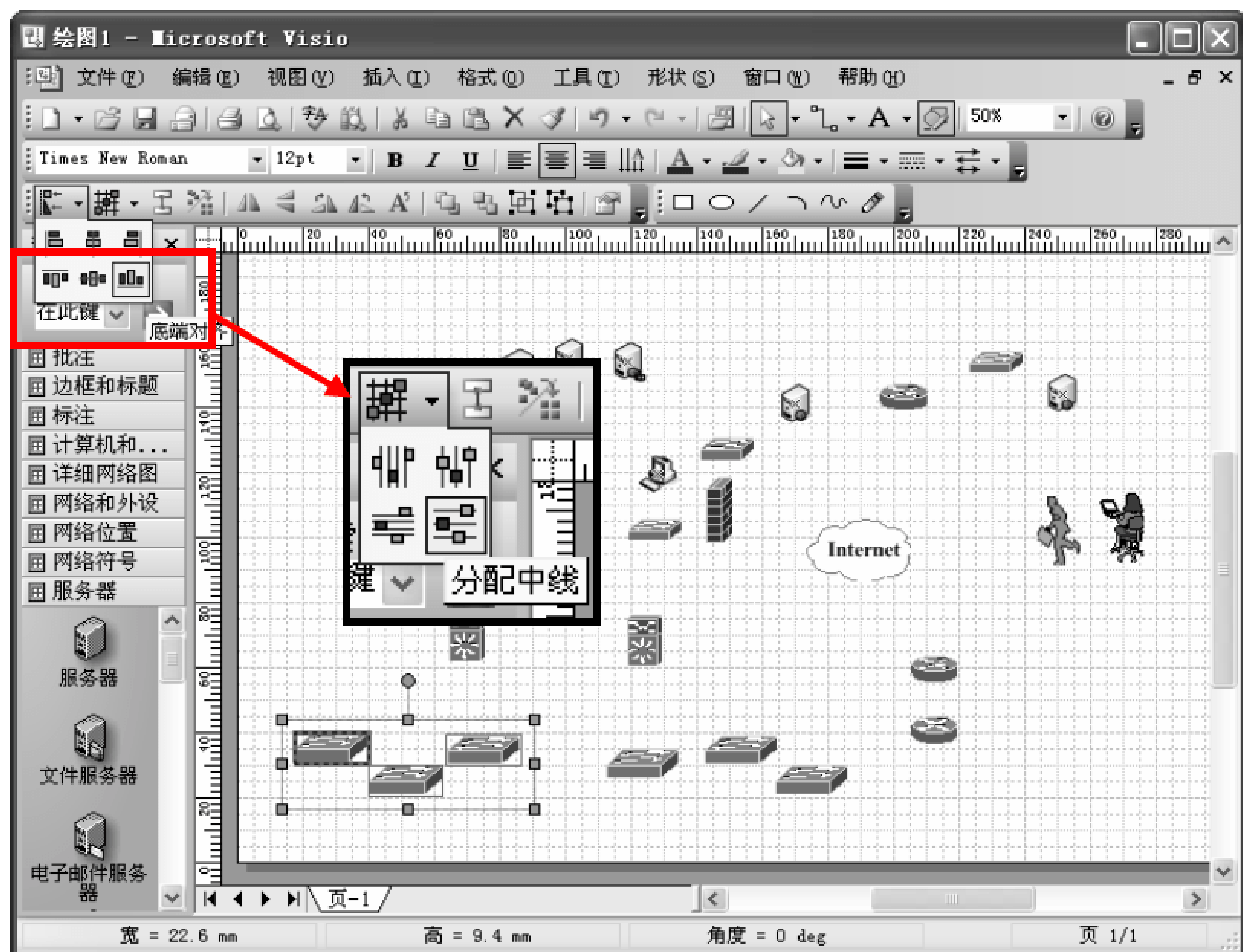


图 1-6　调整设备图标大小及位置

07 所有的图标位置调整好后，可以使用椭圆工具将部分图标圈起来作为一个网络区域使用，可对创建的椭圆右击，在弹出的快捷菜单中选择【形状】➢【置于底层】命令改变其层次，如图 1-7 所示。

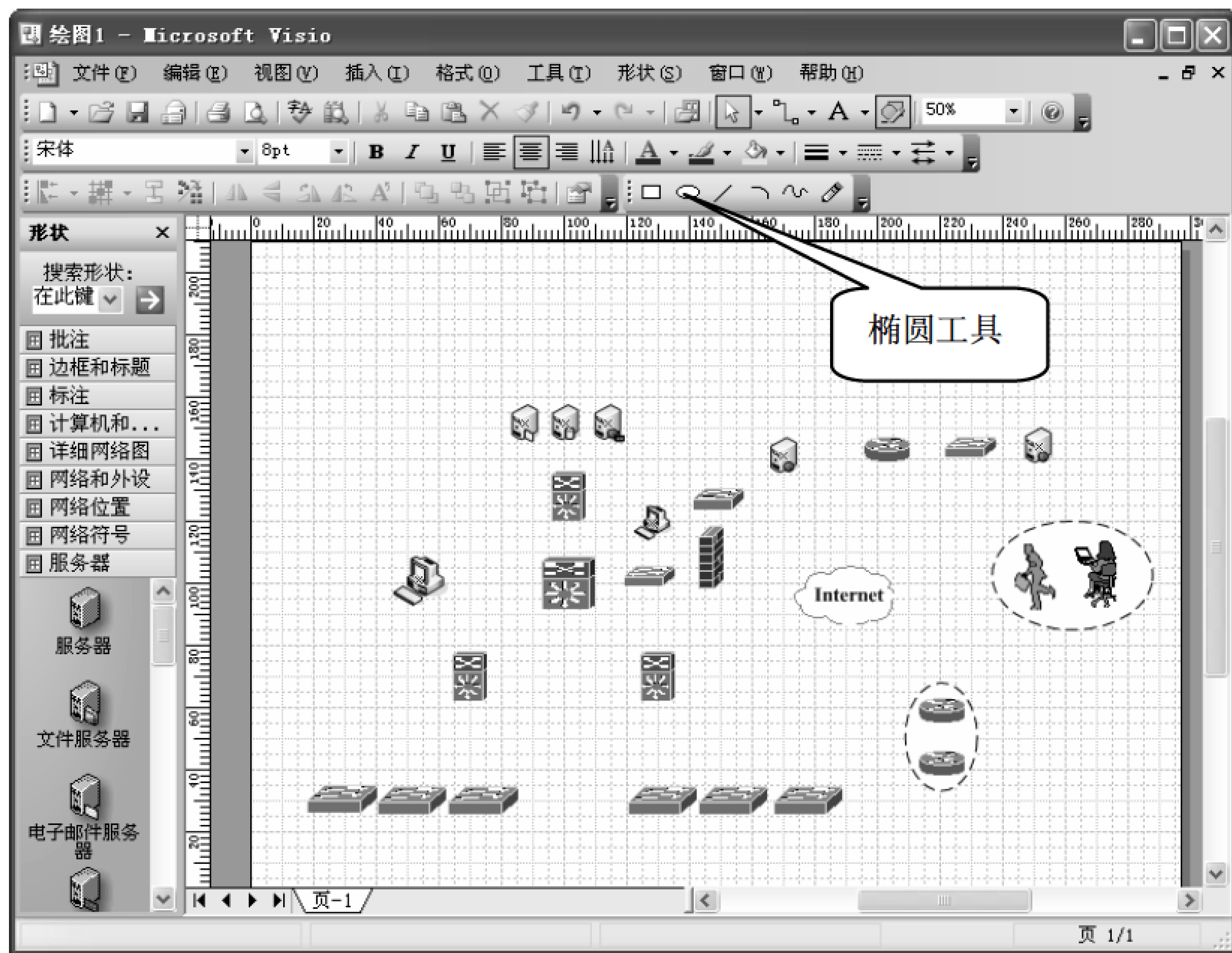


图 1-7　添加椭圆指定网络区域

08 使用【连接线工具】或【线条工具】对设备进行连接。可以根据需求，使用工具栏中的【线型】、【线条粗细】和【线条颜色】等工具对添加好的连接线进行编辑，同时可以选中连接线

右击，在弹出的快捷菜单中选择【形状】➢【置于底层】菜单命令改变其层次，如图 1-8 所示。

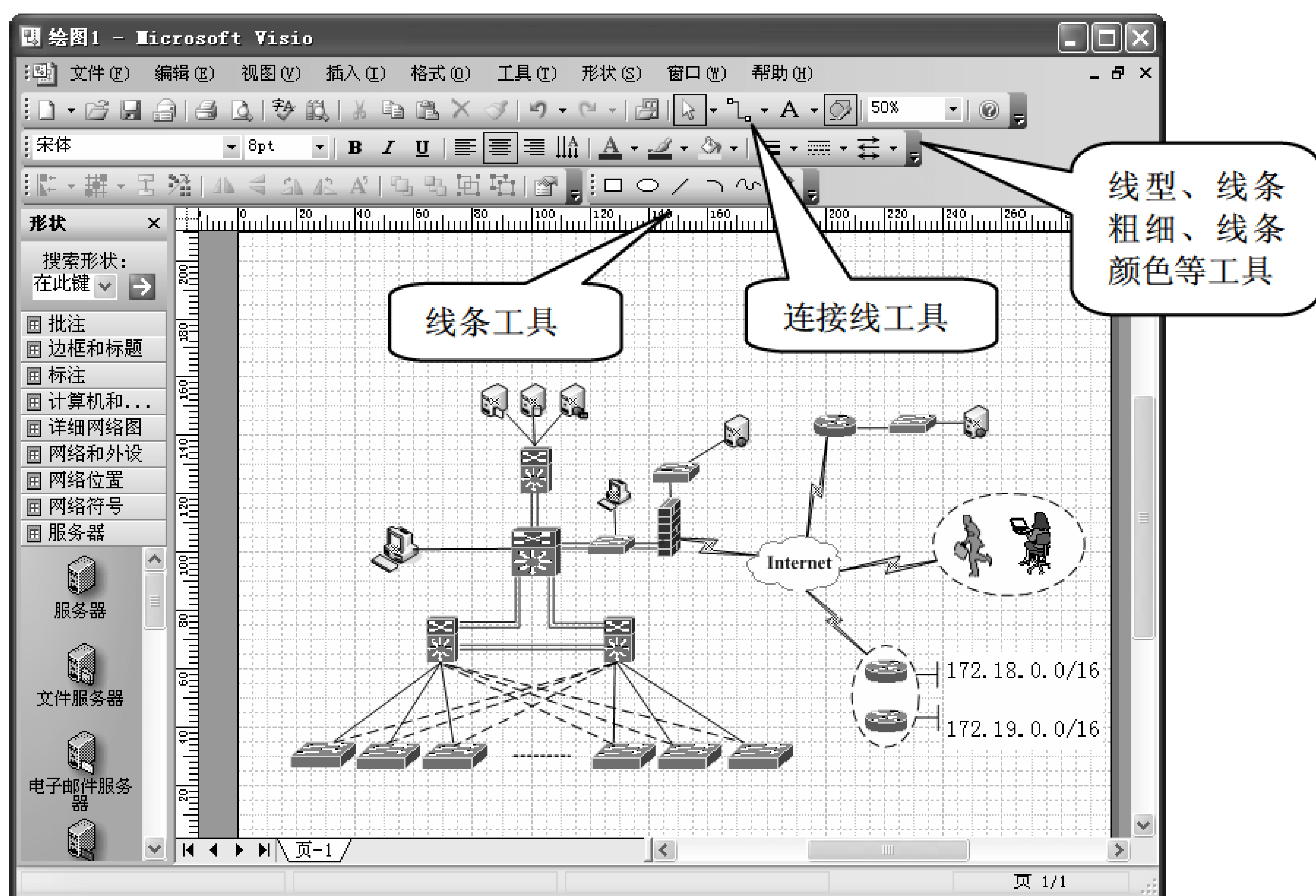


图 1-8　添加连接线

09 使用【文本工具】在图中合适的位置加入文本，输入文本内容，并使用主工具栏中的【格式】工具条编辑文本的字体及大小，然后在图中为文本插入箭头指向，以明确文本的用意，如图 1-9 所示。



图 1-9　添加文本说明

10 在拓扑图左上方加入图注说明，包括设备、线缆类型的说明，如图 1-10 所示。

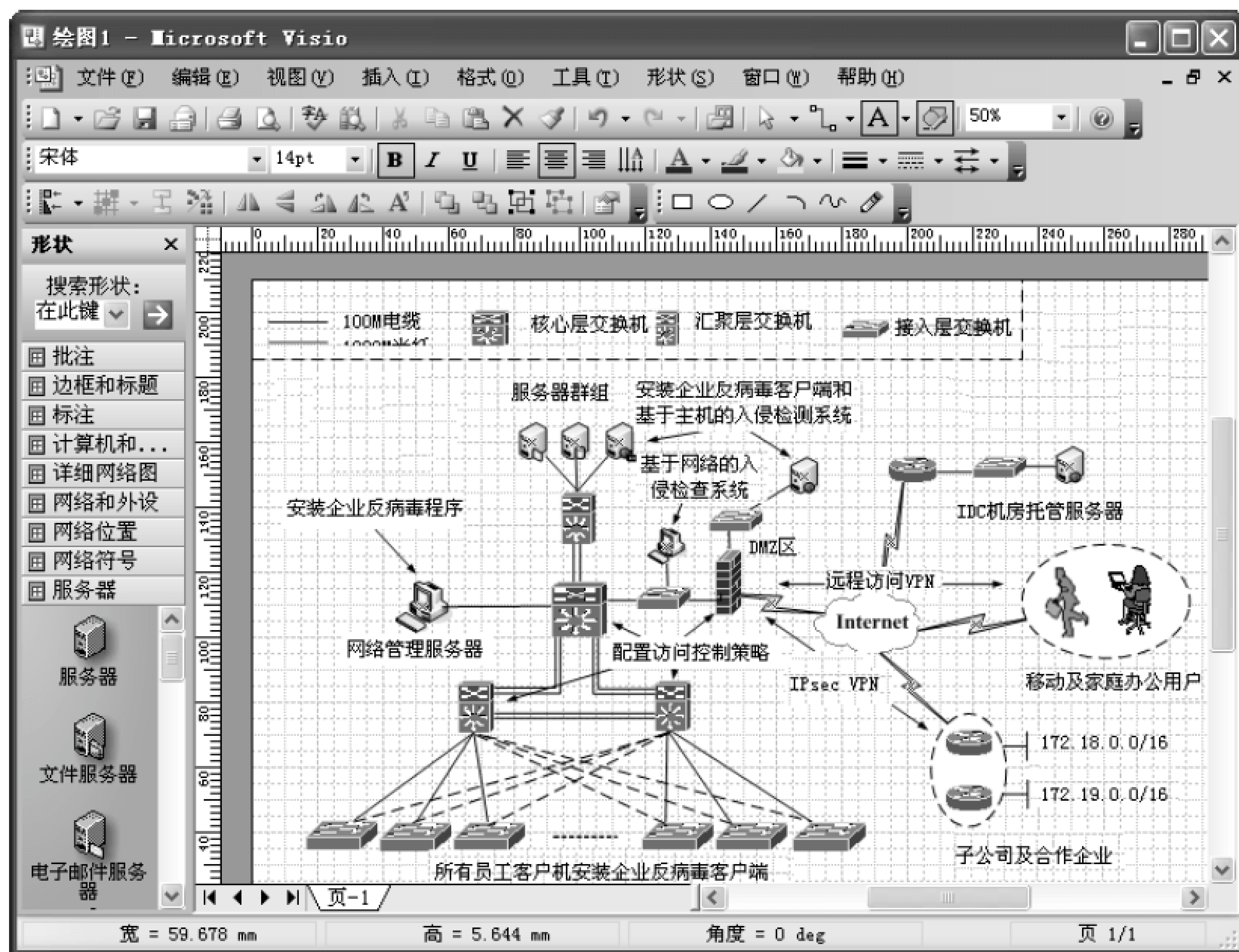


图 1-10　添加图注说明

11 设置完成后，使用 Office 通用办公软件的保存方式将其保存即可，需注意保存格式要选择正确，一般使用 JPG 格式。

1.2　维护企业网络环境

企业网络构建完成投入使用之后，需要保证其持续、稳定的运行，所以需要专业的网络管理维护技术保障。本节将详细介绍网络管理的职能、网络基本信息管理方法及网络管理方案设计等内容。

1.2.1　规范网络管理的范围和任务

计算机网络的规模越来越大，所承担的生活、工作职能越来越繁杂，所以必须要有严格的网络管理体系进行维护，这就需要规范网络管理的范围和管理员的详细职能。下面简单介绍网络管理的工作范围以及网络管理员的工作任务。

网络已经成为人们工作、生活的一部分，很多人没有网络几乎什么都做不了，所以网络管理员需要确保所维护管理的网络能全天 24 小时不间断工作。当网络运行正常时，一切都显得风平浪静，但是一旦网络出现故障，各种疑问、意见、指责接踵而至，网络管理员沦为了众矢之的。所以，作为一名合格的网络管理员，需要掌握完整的、广泛的技术知识，需要熟练操作各种网络设备、操作系统，要能够具备较高的故障发现、恢复能力。

将网络管理员繁杂的工作进行总结，最终可以形成 7 项工作任务：网络基础设施管理、网络操作系统管理、网络应用程序管理、网络用户及其权限管理、网络安全维护、信息存储备份和机房

管理。这 7 项工作任务中的每一项都可以构成一套知识体系。例如网络操作系统管理，根据操作系统类型可以分为 Windows Server 系列、Linux、Unix 等，每一个操作系统又会涉及与其相关的各种服务的配置与管理。又例如信息存储备份，需要了解各种存储设备的调试应用，还要熟练掌握各种数据库的程序调试等。下面对网络管理的 7 项工作任务作详细说明。

（1）网络基础设施管理。网络的运行少不了最基础的硬件设备支持，主要包括网线、交换机、路由器、无线 AP、机柜、电源、计算机、服务器硬件等，这些网络通信中最底层的硬件设备是网络管理员最基本的管理维护对象，需要确保网线布置合理、无损坏，交换机和路由器工作正常、配置准确，机柜牢固、电源稳定，且备用 UPS 电源可用等。

（2）网络操作系统管理。主要是对主流的服务器操作系统的维护，如 Windows Server 2003/2008、Linux、Unix 等。这些服务器中的各类服务，如 IIS、Apache、DNS、DHCP、CA 等，是提供网络应用的主要服务，因此也是网络管理员操作维护的重点。

（3）网络应用程序管理。网络中提供各种实际功能的主要是各种应用程序，如网络管理软件、网络安全软件、办公应用软件、互联网访问软件。用户使用的就是这些软件程序，所以网络管理员要掌握基本的软件安装、故障恢复、卸载等操作。

（4）网络用户及其权限管理。网络中有很多资源供用户使用，或者供不同级别的管理人员操作，为了确保网络的安全可靠，必须严格分配账户身份和权限。

（5）网络安全维护。网络安全是目前网络中的重要问题，合理地利用网络安全设备和技术手段屏蔽网络安全威胁是每一个网络管理员都应当掌握的，需要管理员能够及时升级安全配置，能够熟练地发现安全威胁并将其清除。通常会使用防火墙、防毒墙、入侵检测系统和流量扫描分析程序完成网络安全维护。

（6）信息存储备份。计算机网络中最值钱的不是硬件设备，也不是软件程序，而是数据和信息，任何软硬件设施损坏后都可以重新购置，无非是花一些钱，但是数据和信息一旦丢失，所造成的损失是无法弥补的。所以网络管理员需要对重要的数据和信息进行备份，通常要定期对所有数据进行备份，而对于实时更新改变的数据要实时同步备份。一旦数据损失，要第一时间将备份的数据恢复，最好做到数据零损失。

（7）机房管理。机房是存放重要网络设备的地方，机房的环境对网络设备的稳定运行影响很大，网络管理员应该合理使用机房，确保其物理环境无尘、干燥、防火、防水、防辐射和防盗等。

结合以上内容，可以为企业制定严格的网络管理制度。

1.2.2　项目实战 4：获得网络基本信息

随着企业信息化的发展，网络的规模越来越大，网络中的主机数量越来越多，网络维护越来越难，网络故障解决的时间越来越长，已经影响到了企业的办公效率。作为网络管理员，首先需要解决的就是掌握整个企业网络的规模和设备分布，其次是网络中的服务器信息和主机信息，包括计算机的 IP 地址、MAC 地址、用户以及计算机硬件配置等信息，这些信息可以帮助网络管理员快速定位到主机或者设备的物理位置，从而加快解决故障的速度。因此，经常把网络拓扑图、网络中设备或者主机的分布图、主机的 IP/MAC/用户对应关系以及设备硬件配置等信息称为网络基本信息。

网络拓扑图和网络设备分布图可以通过实地调查获得，但是对于网络中主机的 IP/MAC/用户

对应关系就不是那么容易获取到的，特别是网络中存在 DHCP 服务器时，客户端每次获取的 IP 地址是不同的，要准确地获取每台计算机或者设备节点的基本信息更是难上加难，更别说快速地找到某台计算机，这时候就需要事先制作 IP/MAC/用户映射关系表，当网络出现问题的时候，可以通过数据包分析找到出问题的具体计算机或者设备的 IP 地址或 MAC 地址，通过 IP/MAC/用户关系表找到具体故障主机或者设备的物理位置。

1. 获取网络基本信息的方式

常见的获取网络基本信息方法有两种：工具扫描和走访调查。

1）工具扫描

面对大量的客户端，工具扫描是个不错的方法。工具扫描是指在局域网中任意一台计算机上安装扫描工具，然后扫描局域网所有正在运行的计算机获取网络基本信息。

通常可以使用的扫描工具比较多，有专门进行网络扫描的小程序，也可以使用企业网络管理平台自带的扫描功能。第 16 章介绍的 SolarWinds 工具就是使用得比较多的一款网络管理工具集程序。

2）走访调查

面对大量的客户端，工具扫描可以统计出全部正在运行的计算机或者网络设备的网络基本信息，但是每台计算机或者网络设备的物理位置等信息是无法统计到的，这些还必须依靠人工走访调查来进行统计，以完善网络基本信息。

2. 使用 Windows 系统内置工具——ipconfig

ipconfig 是内置在 Windows 系统的 TCP/IP 应用程序，用于查看计算机本地网络适配器的计算机名称、IP 地址和 MAC 地址等 TCP/IP 信息。ipconfig 主要用于手工检查计算机的 IP 地址配置。另外在 DHCP 服务器存在的网络中，ipconfig 命令还可以用于释放和获取 IP 地址信息。

1）查看本机的 IP 地址信息

使用 ipconfig 命令查看 IP 地址信息的具体操作步骤如下。

01 选择【开始】➢【运行】命令，弹出【运行】对话框，在【打开】文本框中输入 cmd 命令，单击【确定】按钮，如图 1-11 所示。

02 弹出命令提示符窗口，在其中输入 ipconfig 命令，按 Enter 键确认，显示出 Windows IP Configuration 信息，包括 IP Address（IP 地址）、Subnet Mask（子网掩码）和 Default Gateway（默认网关）等，如图 1-12 所示。



图 1-11　【运行】对话框



图 1-12　在命令行使用 ipconfig 命令

2）查看本机的 MAC 地址

在命令提示符窗口中，输入 ipconfig /all 命令，按 Enter 键确认，显示出“Ethernet adapter 本地连接”信息，包括 Description（描述）、Physical Address（物理地址）、DHCP Enabled（DHCP 服务器是否开启）、IP Address（IP 地址）、Subnet Mask（子网掩码）、Default Gateway（默认网关）等，图 1-13 所示。

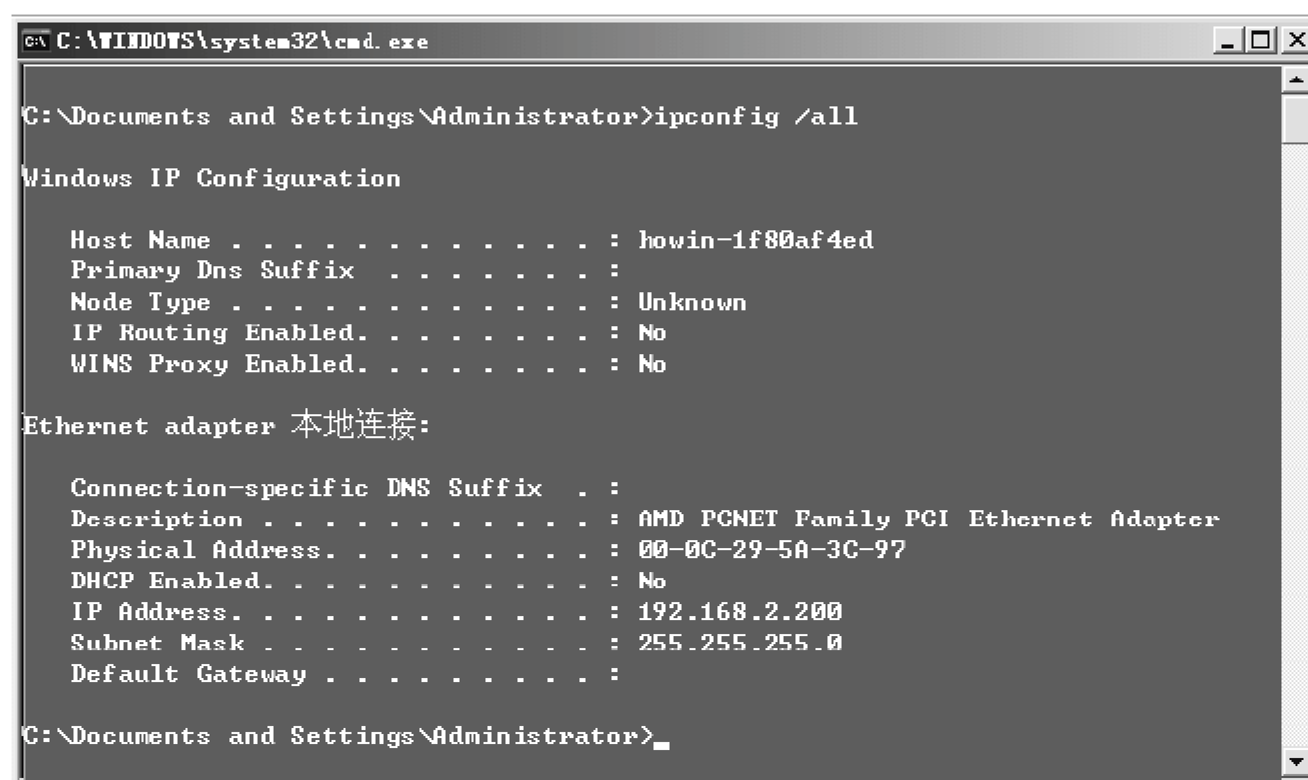


图 1-13　在命令行查看本机 MAC 地址

3）释放本机的 IP 地址

在命令提示符窗口中，输入 ipconfig /release 命令，按 Enter 键确认，会看到本机的 IP 地址被释放掉，如图 1-14 所示。

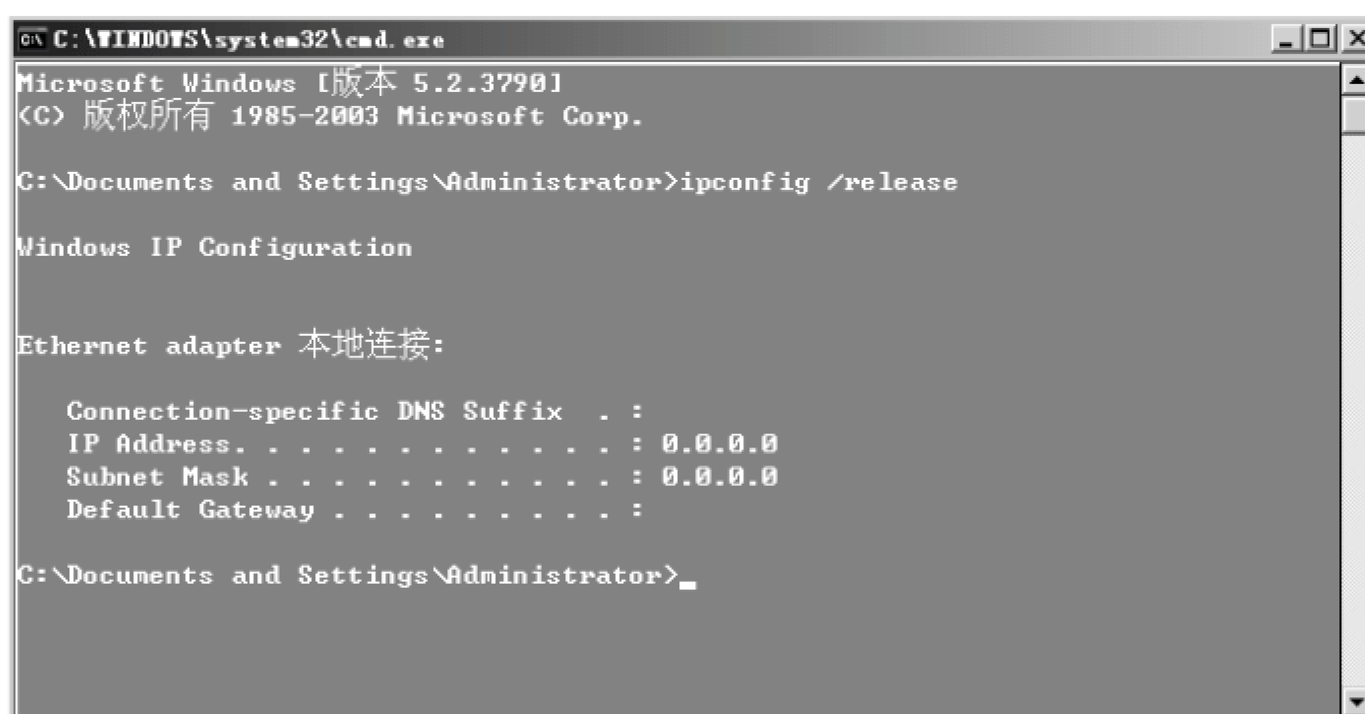


图 1-14　释放本机 IP 地址

4）从 DHCP 服务器上重新获取 IP 地址

在命令提示符窗口中，输入 ipconfig /renew 命令，按 Enter 键确认，会看到本机重新获得新的 IP 地址，如图 1-15 所示。

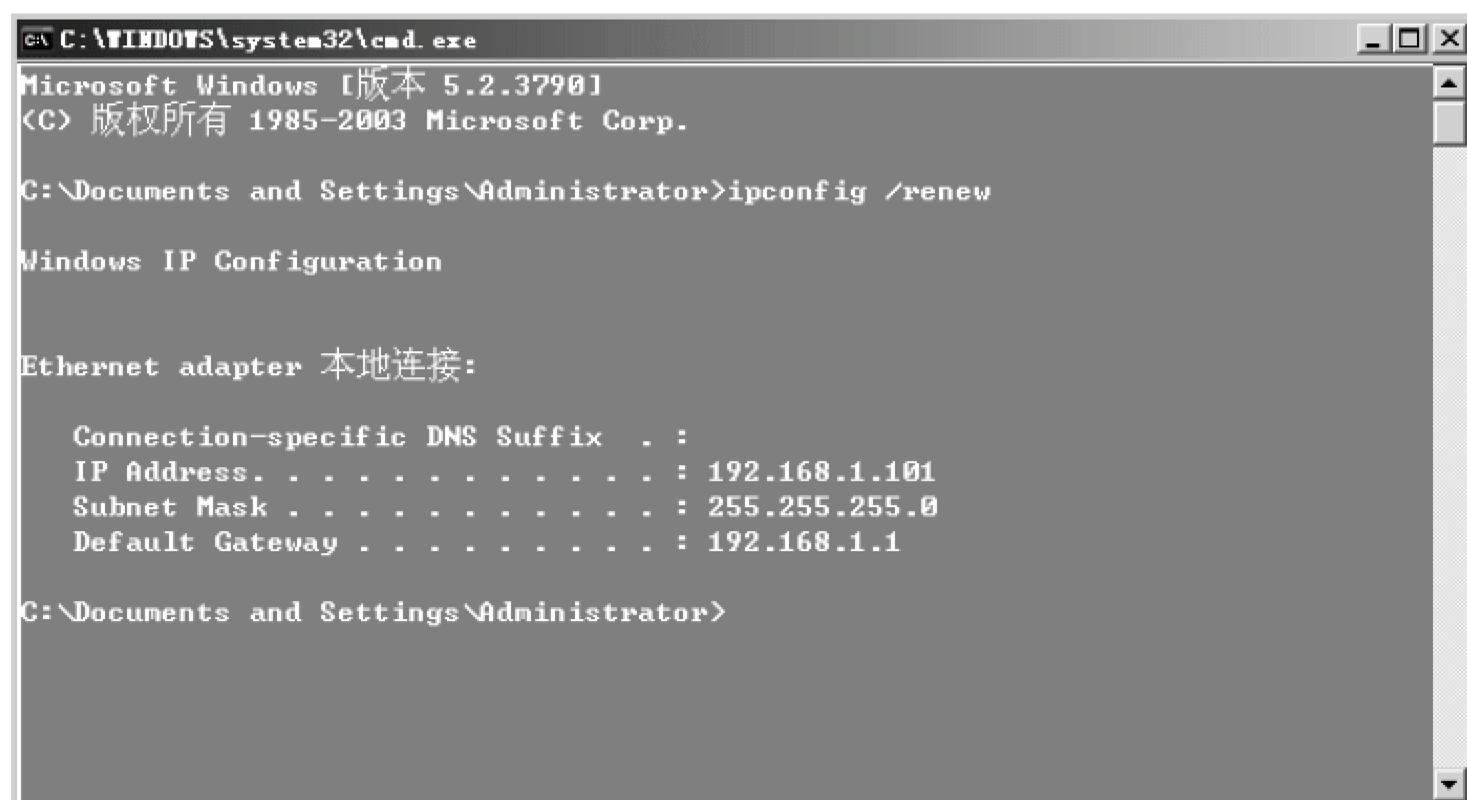


图 1-15　重新获得 IP 地址

3. 使用 MAC 扫描器生成基本信息库

MAC 扫描器是一款绿色共享软件，主要功能是扫描网络中计算机等设备的 IP 地址、MAC 地址、计算机名称和工作组名称等信息。该软件可以帮助管理员快速地搜集网络的基本信息。使用 MAC 扫描器建立基本信息库的具体操作步骤如下。

01 打开 MAC 扫描器，在【IP 范围】文本框中输入要扫描 IP 地址的范围，本案例扫描的 IP 范围是 192.168.1.1 至 192.168.1.255，单击【开始】按钮，如图 1-16 所示。

02 MAC 扫描器自动扫描，并显示扫描进度及结果，扫描结束后单击【保存】按钮，如图 1-17 所示。



图 1-16　配置扫描范围



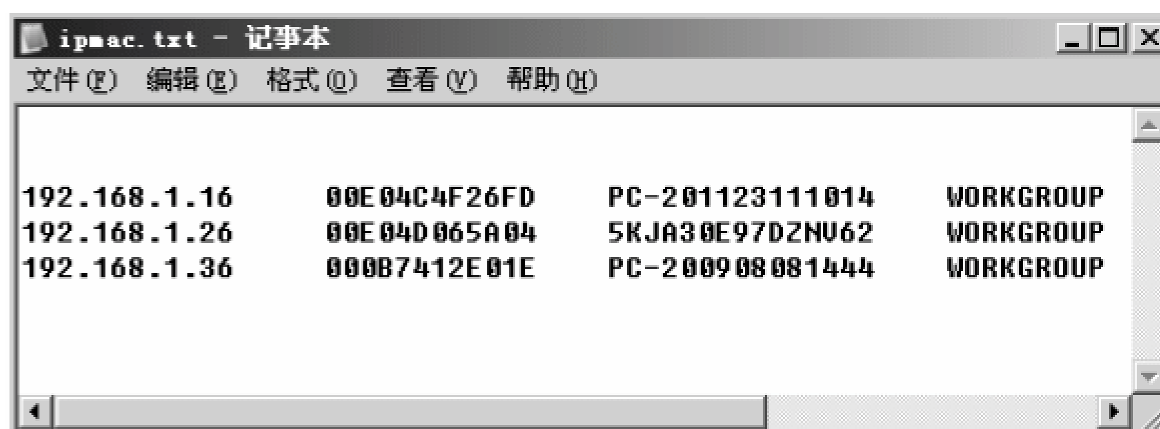
图 1-17　获得扫描结果

03 弹出【保存】对话框，在【文件名】文本框中输入文件名 ipmac，保存文件类型为 txt，单击【保存】按钮，如图 1-18 所示。

04 打开 ipmac.txt 文件，可以看到搜集到的 IP 地址、MAC 地址、计算机名和工作组名称等网络基本信息，如图 1-19 所示。



图 1-18 【保存】对话框



192.168.1.16	00E04C4F26FD	PC-201123111014	WORKGROUP
192.168.1.26	00E04D065A04	5KJA30E97DZNV62	WORKGROUP
192.168.1.36	000B7412E01E	PC-200908081444	WORKGROUP

图 1-19 保存结果

05 网络管理员需要将每个 IP 地址的使用者和设备的物理位置填入该文件以完成基本信息库的建立，如图 1-20 所示。



IP地址	MAC地址	计算机名称	工作组	员工姓名	设备位置
192.168.1.16	00E04C4F26FD	PC-201123111014	WORKGROUP	王小兵	三楼行政办公室
192.168.1.26	00E04D065A04	5KJA30E97DZNV62	WORKGROUP	聂小帅	二楼人事办公室
192.168.1.36	000B7412E01E	PC-200908081444	WORKGROUP	王红	二楼人事办公室

图 1-20 修改扫描结果构成完整信息库

1.2.3 项目实战 5：设计网络管理实施方案

近年来网络管理技术越来越受重视，很多企业开始加强网络管理。对于一个现实的网络环境，如何实施网络管理呢？下面结合一个网络管理案例进行需求分析、方案设计及项目实施的讲解。

1. 项目介绍

在进行网络管理分析之前首先要了解企业概况、网络现状等信息。下面是案例企业的简介及网络概况。

1）公司简介

某 IT 企业成立于 2004 年，主要从事软件开发及电子产品生产。在这 7 年时间里企业有了飞速的发展，除了北京总部外，在全国各地还有多家子公司。在北京总部，员工数量比较多，有 200~300 名，被分配在 4 个工作区。除此之外还有一部分员工经常出差需要移动办公。在各个子公司员工数量相对较少，主要进行产品加工及分销工作。

2）网络现状

网络现状可以总结为以下几点。

（1）全部使用 Cisco 产品，并使用了三层交换机。

（2）总公司与子公司业务量比较少，采用 VPN 连接。

（3）对于移动办公用户和家庭办公用户使用远程访问 VPN 的方式访问企业服务器。

（4）在总公司内配置了供员工访问的 FTP、Web、数据库等服务器。

（5）为了宣传企业形象，在公共网络 IDC 机房托管一台服务器，用于发布企业官方网站、OA 及邮件系统。

（6）企业总部用户使用全交换网络互连，为了减少广播使用 VLAN 隔离。

（7）企业总部出口采用 10M 光纤，子公司一般采用 4M 宽带。

3）网络拓扑

根据网络环境绘制如图 1-21 所示的网络拓扑图。

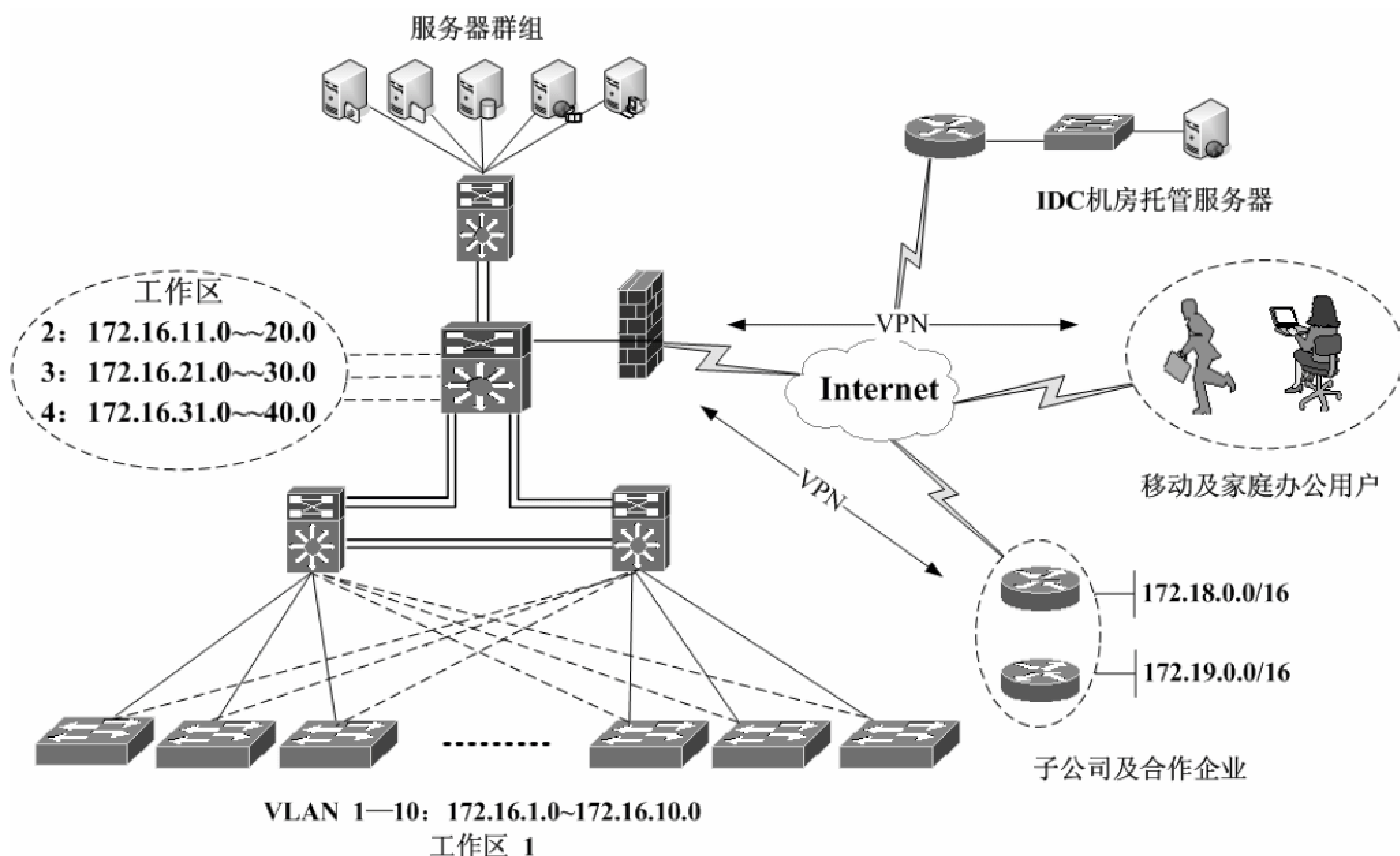


图 1-21　企业网络拓扑图

4）网络管理现状

企业网络环境已成规模，但是网络管理依然落后，目前存在的网络管理问题有以下几点。

（1）网络内经常出现地址冲突现象，广播流量过大。

（2）虽然出口带宽为 10M 光纤，但是内网员工访问公网时网速依然不容乐观。

（3）企业网络故障恢复时效低，经常会因为网络故障影响公司业务及员工办公。

随着业务的扩展，企业对网络环境的可靠性、稳定性要求越来越高，必须完善现有网络的管理体系。

2. 需求分析

结合网络管理现状，做出如下分析。

1）网络内经常出现地址冲突

造成企业内频繁出现地址冲突的原因有以下两点：其一，现在使用移动办公设备的员工越来越多，新增的移动设备在没有充足 IP 地址的情况下，会被设置成其他固定台式机的 IP 地址，台式机地址被占用后为了能联网会更改其 IP，可能又和其他主机地址冲突，这样循环下去地址冲突现象会越来越多。其二，木马病毒一直是计算机使用者头痛的程序，例如 ARP 病毒就可以造成局域网地址冲突，如果一台计算机感染，此病毒会迅速向网络中的其他主机发送地址欺骗信息，造成这些主机出现地址冲突现象，而且这类病毒极易传染。

解决办法：要解决地址冲突可以从两方面考虑，首先是地址不足，管理员在进行地址分配时可以多做冗余，例如 50 人的部门可以分配拥有 126 个可用 IP 的子网，同时再配置 DHCP 动态地址分配服务器，所有新增主机全部采用动态 IP 地址。其次所有关键设备，如路由器、交换机全部配置 IP+MAC+端口的地址绑定，所有主机也可以执行地址绑定的脚本文件。

2）广播流量过大

广播流量过大主要有两个原因，其一是广播域太大，其二是由病毒或木马引起的。本方案中已经做了较细致的 VLAN 划分，广播域已经被缩小，可以不考虑广播域的问题。病毒和木马都具有较强的传染性，当企业内的某台主机感染病毒或木马后，可能会向局域网内的其他主机发送大量广播信息，以实现网络攻击与传染。

解决办法：通过网络性能检测工具实时检测广播源，并及时隔离清除威胁。

3）网速不容乐观

目前网络出口带宽已经有 10M 光纤，这对于一般企业来说已经够用了，所以造成网速较慢的原因可以从 3 个方面考虑。其一，局域网带宽被大量广播消耗掉了，很多内部网络还都是使用 100M 双绞线，如果短时间内出现了大量的广播流量，就会出现网络拥塞，导致网络访问请求延迟。其二，有个别用户在使用下载工具或观看在线视频，10M 带宽资源已经算是充足，但是依然有个限度的；如果网络内出现大量的视频或文件下载流量，必然会导致其他用户服务抢不到出口带宽。其三，网络攻击阻碍互联网访问，如拒绝服务式网络工具，可以拥塞公网出口，使内网请求信息无法正常转发。

解决办法：可以在网络内架设流量监控系统，实施监控所有网络流量，通过监控系统可以分析出占用带宽的数据源，然后再使用网络管理工具断开这些主机的网络或限制其流量。同时还可以在网络设备上作访问控制，特别要限制视频流量和特殊网站流量通过出口设备。

4）网络故障频繁

企业网络环境相对复杂，从企业建成发展至今，网络设备随着业务扩充不断地增加，新旧设备混合，再加上管理混乱，网络故障才会频繁发生。如果网络环境的负载不能满足通信的要求，过多业务流量会让网络处于超负荷工作状态，如网络设备的背板带宽、传输速率、CPU 性能等。如果能在网络隐患，还处于萌芽状态时就将其扼杀，网络故障自然就少了。

解决办法：要经常进行网络性能分析，处于关键位置的设备需要有专门的程序实时地监控其运行状态、性能指数，在超出网络负载之前要做好升级改造工作。

5）故障恢复时效低

故障恢复时效低和不健全的网络管理有直接关系，企业飞速的发展忽略了网络管理的重要

性，一直采用传统的管理方式，即便是加入了一些网络管理设备，也因网络管理水平的限制而成为摆设。传统的网络管理几乎采用人工式的反应，故障发现之前很难察觉，故障发生后才会被发现，而这时故障，已经造成了一定的损失，恢复起来相对难度会大一些，单是排查故障原因就需要耗费很多时间。

解决办法：建立网络管理平台，实施监控网络状态。通过网络管理平台准确找出故障点与原因，进行针对性的故障恢复。

通过以上需求分析可以对网络实施相应的改造，具体网络改造内容可以总结为以下几点。

（1）建立网络基础信息档案，包括网络拓扑结构、设备数量、地址配置、功能实现、对应表（MAC+IP+端口+用户）等，以帮助管理员掌握网络，并为解决网络故障提供辅助资料。

（2）搭建网络管理平台，做到对整个网络的实时监控。

（3）对重点网络设备作性能的实时监测。

（4）对企业内网服务器和 IDC 机房托管服务器采用远程服务器监控程序，进行维护。

（5）架设网络流量监测分析程序，实时监控网络流量，以方便发现网络故障隐患以及查找故障原因。

（6）运用安全的网络管理协议。

实施改造后企业网络拓扑结构没有太大改变，但是网络管理能力得到了极大的提升，改造后的网络拓扑图如图 1-22 所示。

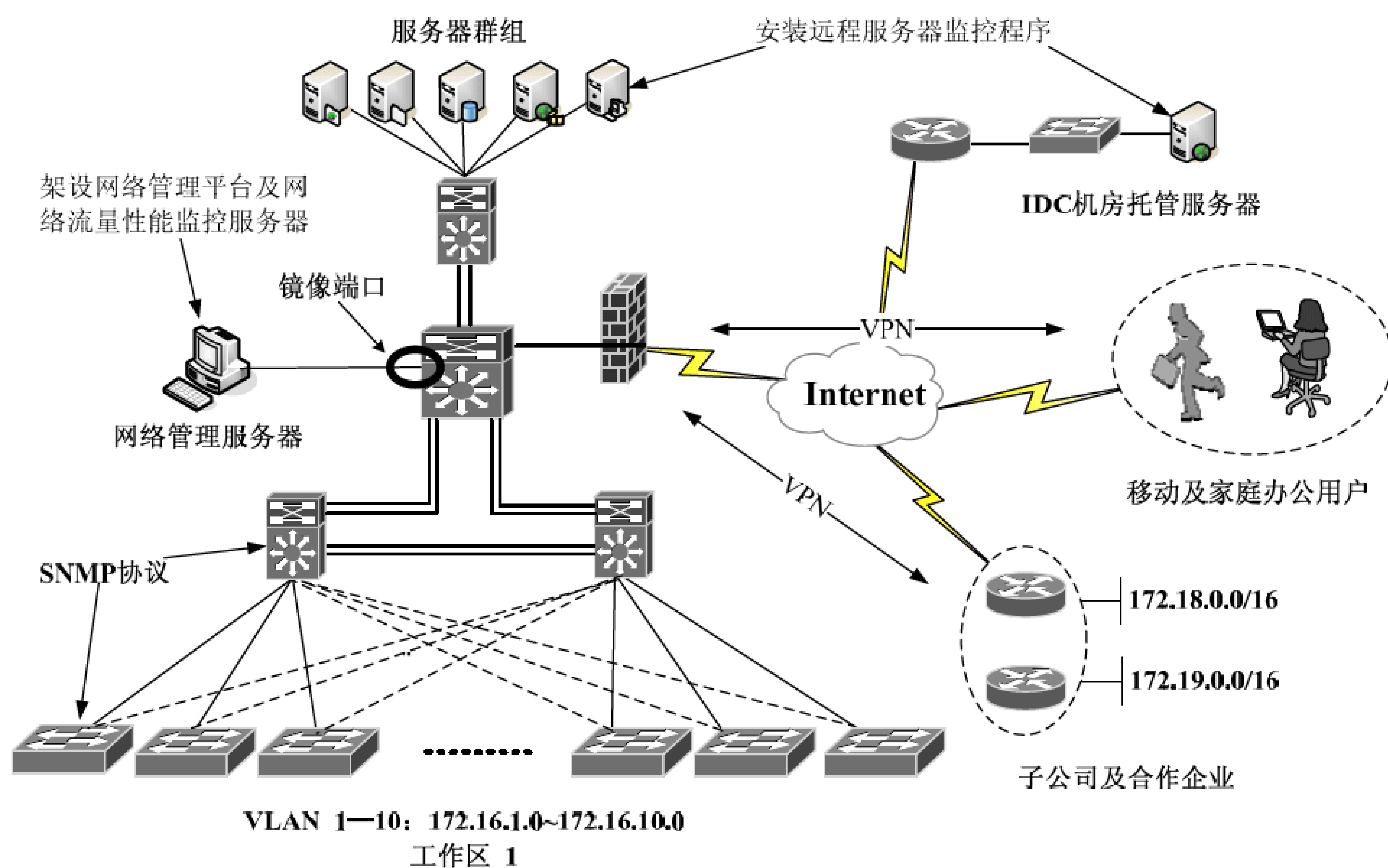


图 1-22　调整后的网络拓扑图

在网络中加入一台专门的网络管理服务器，用于安装网络管理平台和网络性能监控服务器等程序。给所有服务器安装远程服务器管理程序的客户端。为了使网络管理服务器可以监控全网流量，在所有交换机做镜像端口，流量镜像到网络管理服务器方向。在所有网络设备和计算机开启 SNMP

服务，配置安全的共同体，并配置必要的 Trap 自陷消息。

3. 项目实施流程

项目要采用分步实施的方式完成。结合上文的需求分析，网络管理方案可以分为以下 6 个操作步骤。下面分别作详细介绍。

1）获得网络基本信息

获取网络基本信息是管理整个网络的根本。作为网络管理员，想要高效地完成网络管理任务，首先要了解当前的网络结构，获取基本网络信息，如网络规模、主机分布、IP/MAC/主机名/用户对应关系、设备数量及分布、设备型号及配置、主机及服务器（硬件）配置等信息。如果网络出现问题，就可以根据事先掌握的信息快速地找到故障点，并加以解决。

获取网络基本信息可以通过现场调查和网络扫描工具两种方式来实现。获取网络基本信息难度并不大，但是工作量确实不小，使用网络扫描工具可以快速地获得需要的 IP、MAC、计算机名等对应信息，但还是有一些东西是无法用工具扫描到的，如部门人员分配，这些无法扫描到的信息需要通过现场调查走访的方式获取。

常用的网络扫描工具有 IPMaster（IP 地址管理工具）、MAC 地址扫描器等。

获取到网络基本信息后，可以建立网络基本信息库，此信息库可以使用表的方式体现。表 1-8 和表 1-9 为给出的参考样表。

表 1-8　员工网络地址统计表

姓名	部门	办公室	计算机名	IP 地址	MAC 地址	机器配置	联系电话	其他

表 1-9　网络设备信息统计表

网络设备	地理位置	设备名	硬件配置	功能作用	地址配置



网络基本信息统计表要根据企业环境需求而进行设计，一定要做到准确、结构清晰、易查找。

2）搭建网络管理平台

企业内的网络设备比较多，链路连接也比较复杂，一旦发生网络故障，管理员很难在第一时间找出故障原因，需要经过长期的排查。而在企业里一分钟的业务中断都有可能造成巨额损失，必须要尽量缩短故障恢复的时间。想要缩短故障恢复的时间，需要有良好的故障恢复能力，同时也需要有更好的方法查找网络故障原因。

网络管理平台，又叫网络运维系统。通过该系统可以实时获取网络拓扑信息和网络设备的配置、性能信息，如果设备出现异常会通过各种图表进行显示，同时还可以根据阀值进行报警提示。这样一来网络性能指标超过阀值时管理员就会知道，通过调试可以避免严重的网络故障发生。如果网络故障已发生了，也可以通过网络管理平台清晰地找到故障点和故障原因。

搭建网络管理平台需要在网络管理服务器上安装管理平台软件，并在所有被监控的设备上运行 SNMP 协议。搭建网络管理平台可以按照图 1-23 所示的拓扑图实施。

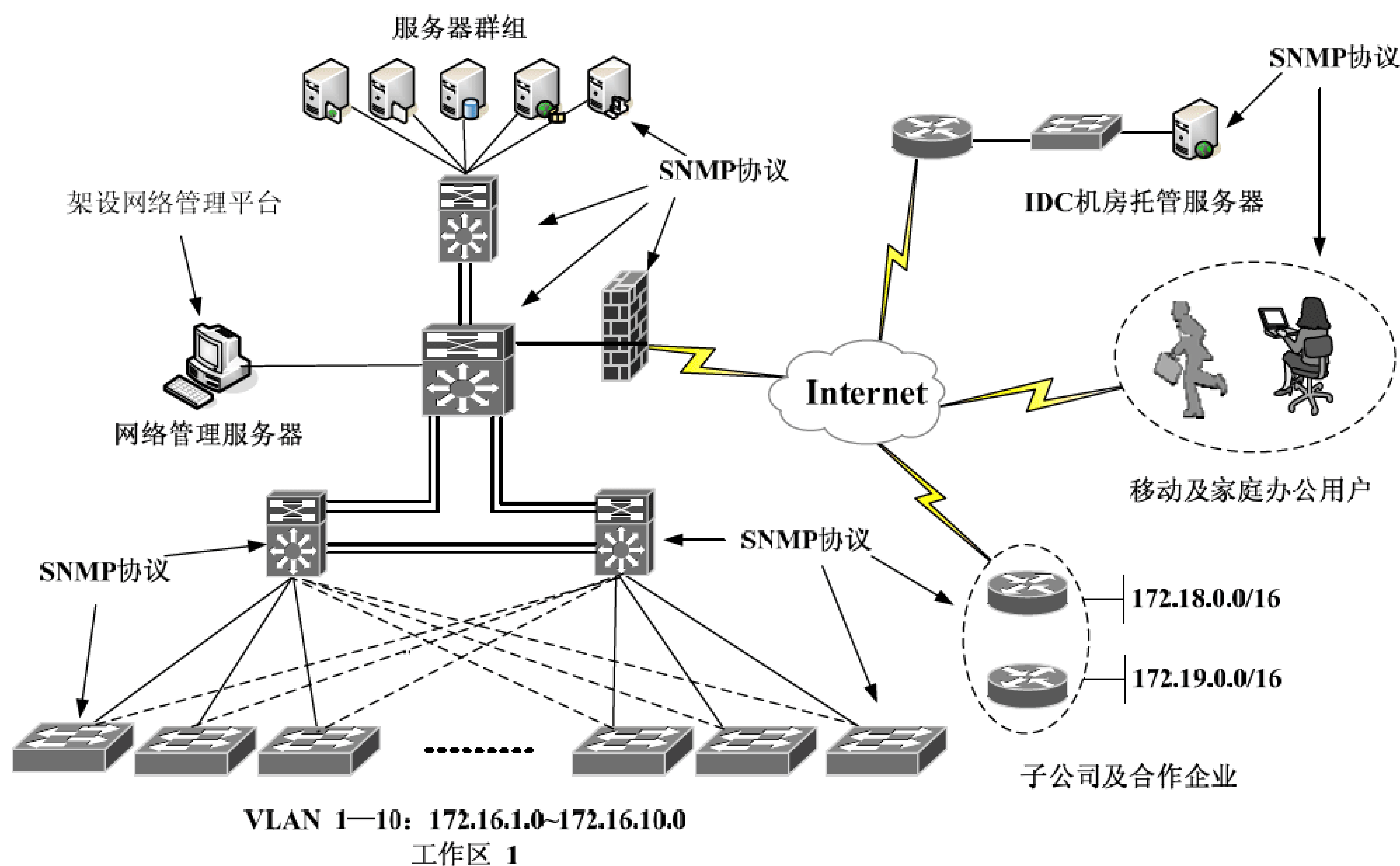


图 1-23 搭建网络管理平台后的拓扑图

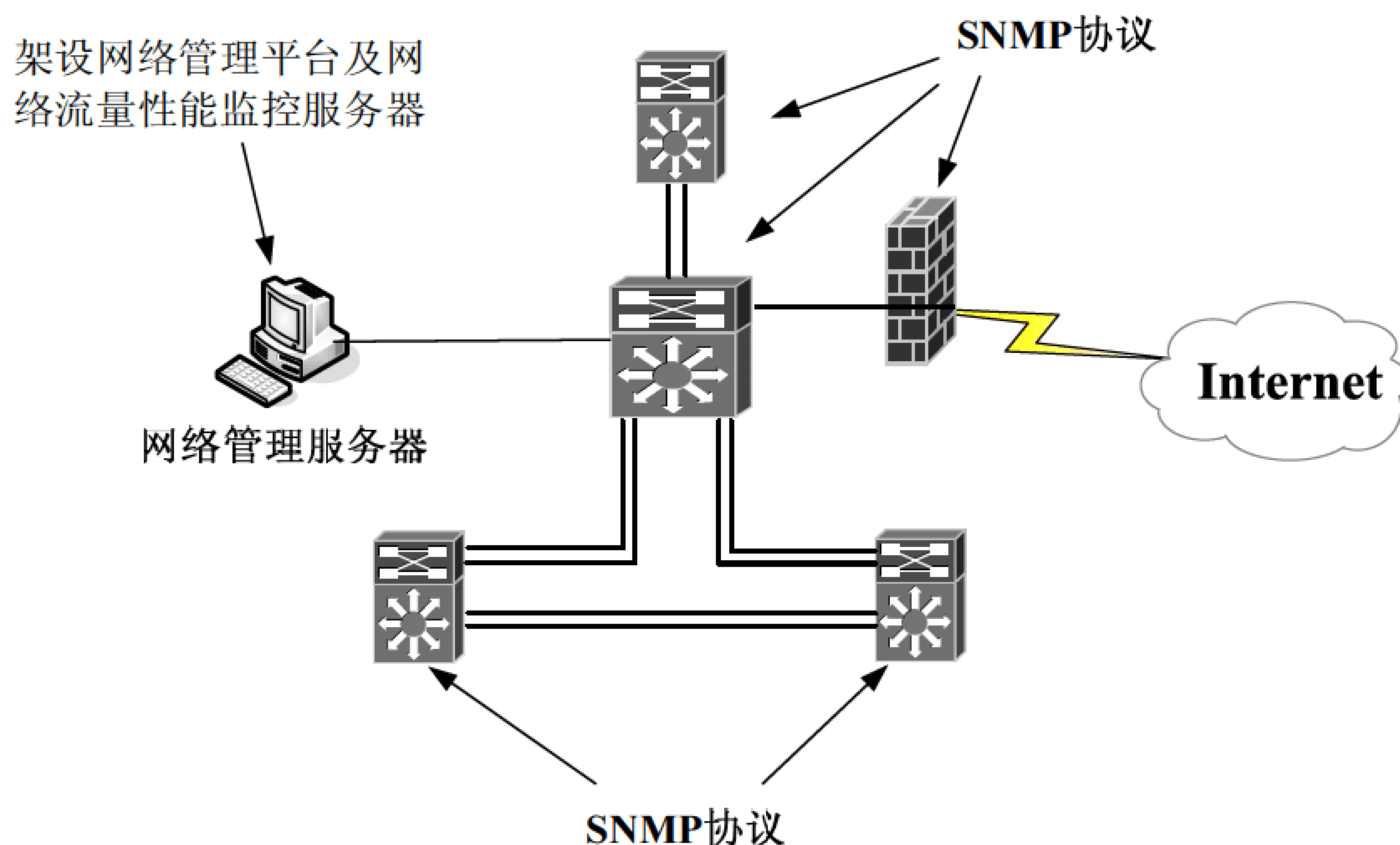
目前用得比较多的网络管理平台有 Spiceworks、WhatsUp Gold、HP OpenView、IBM Tivoli NetView，除此之外还有很多类似软件，但是大部分软件在使用上都大同小异。

3）监控重点网络设备

企业网络里的个别设备处于关键位置，一旦损坏将对整个网络的运作造成巨大的影响，所以要采用专门的工具监测这些设备的运行状态，一般监测的有 CPU、出入流量统计等信息。

很多工具里面都包含有这项功能，如网络管理平台和网络流量性能监控系统。不过这里还是需要强调一下这项工作的重要性。除了以上程序自带该项功能外，还可以使用 SolarWinds 工具，该工具是一套非常全面的网络管理工具，可以实现很多网络管理需求，其中值得注意的是该工具专门嵌入了 Cisco 设备管理功能。对网络设备进行监控时不需要过多操作，只要确保设备开启 SNMP 协议即可。

根据设计可以做出如图 1-24 所示的调整。



某公司网络工程图例

图 1-24　监控重点设备拓扑

4）实现服务器远程控制

企业的大部分工作都需要内外网服务器作支撑，所以企业内网络服务器和 IDC 机房托管服务器稳定性至关重要，必须要实时监控这些服务器的性能，并且要有安全可靠的远程管理手段完成服务器的监控与配置。

传统的方式是采用 Windows 自带的远程桌面连接功能，这样做虽然可以直观地操作远程服务器，但是安全性较弱，任何主机只要知道地址和账户都可以连接，并且这样只能做到对远程服务器的控制，却不能实时获取远程服务器的性能信息，需要另找程序监测性能。

除了传统方式外，还可以采用 SSH、VNC 和其他专业远程服务器管理工具，这些方法一般都带有较为严格的认证加密手段，部分方法除了指定的管理服务器外，其他主机很难对服务器进行管理控制。可按照图 1-25 所示的拓扑图实施服务器远程控制。

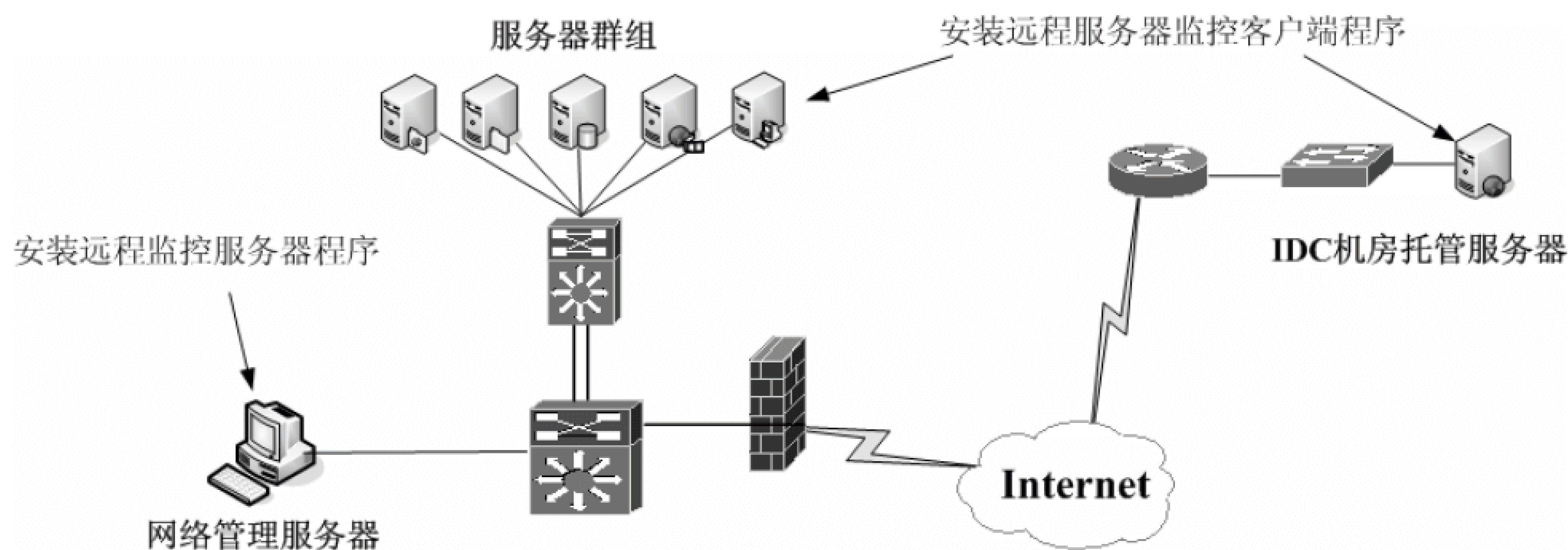


图 1-25　服务器远程监控的拓扑图



提　示

对于 IDC 机房的托管服务器，在实施远程管理时可能会产生特殊的管理数据流，这些流量需要被出口的防火墙设备转发，应注意防火墙的访问控制策略。

5）加强员工网络安全管理意识

在企业网络中，管理员做得最多的工作是为普通用户作机器维护。由于普通员工的计算机使用水平不一样，很多用户不能合理地使用计算机，一旦遇到计算机故障就不知道该如何处理。所以作为管理员，一定要具有较高的单机故障维护能力，多准备一些故障维护盘。

造成网络中单机维护工作过多的原因除了员工操作水平不高外，与单机的安全防护能力弱也有直接关系。很多员工在使用计算机时不注意个人主机的安全，没有杀毒软件和漏洞检测软件，“裸机”上阵的很多，这些机器极易感染病毒木马，一旦被网络攻击者利用，很有可能成为威胁整个网络的隐患。

所以在实施网络管理改造中，可以适当对员工进行计算机基础应用培训，让员工安全使用计算机，并掌握独立解决小故障的能力。

6）故障检测与分析

在网络管理中，经常出现网速慢、地址冲突频繁、出现大范围网络攻击等现象，这些故障一般都不是硬件造成的，想要找到故障原因，难度很大，目前最有效的方法就是通过分析网络数据流查找异常信息流。

当机器感染了 ARP 病毒后，会迅速向全网发送地址欺骗信息，通过网络流量监测分析工具可以清晰地看出是哪台主机在发送大量的 ARP 信息，结合之前统计的网络基本信息可以很快地找到感染病毒的主机用户，让其进行病毒的查杀。

如果网速变得很慢，也可以通过流量监测分析工具对全网进行流量分析，找出比较占用带宽的数据流。通过查看单位时间内哪台主机接收的数据包最多，就可以判断出带宽严重浪费的原因。

每种网络故障都有独特的网络异常流量，这里不再作过多的介绍。这里有另外一个问题需要考虑，网络环境中的流量这么多，想要实现流量监测就必须让所有流量通过网络流量性能监控服务器，广播流量还好说，但是跨网段流量和单播流量如何确保都流经流量性能监控服务器呢？这需要

在所有网络设备上作一项技术配置——镜像端口。通过镜像端口技术，可以把交换机多个端口的流量分别做一份数据镜像转发到镜像端口，所有的镜像端口都朝着网络流量性能监控服务器方向配置，就可以实现全网流量监控。

根据设计可以做出如图 1-26 所示的调整。

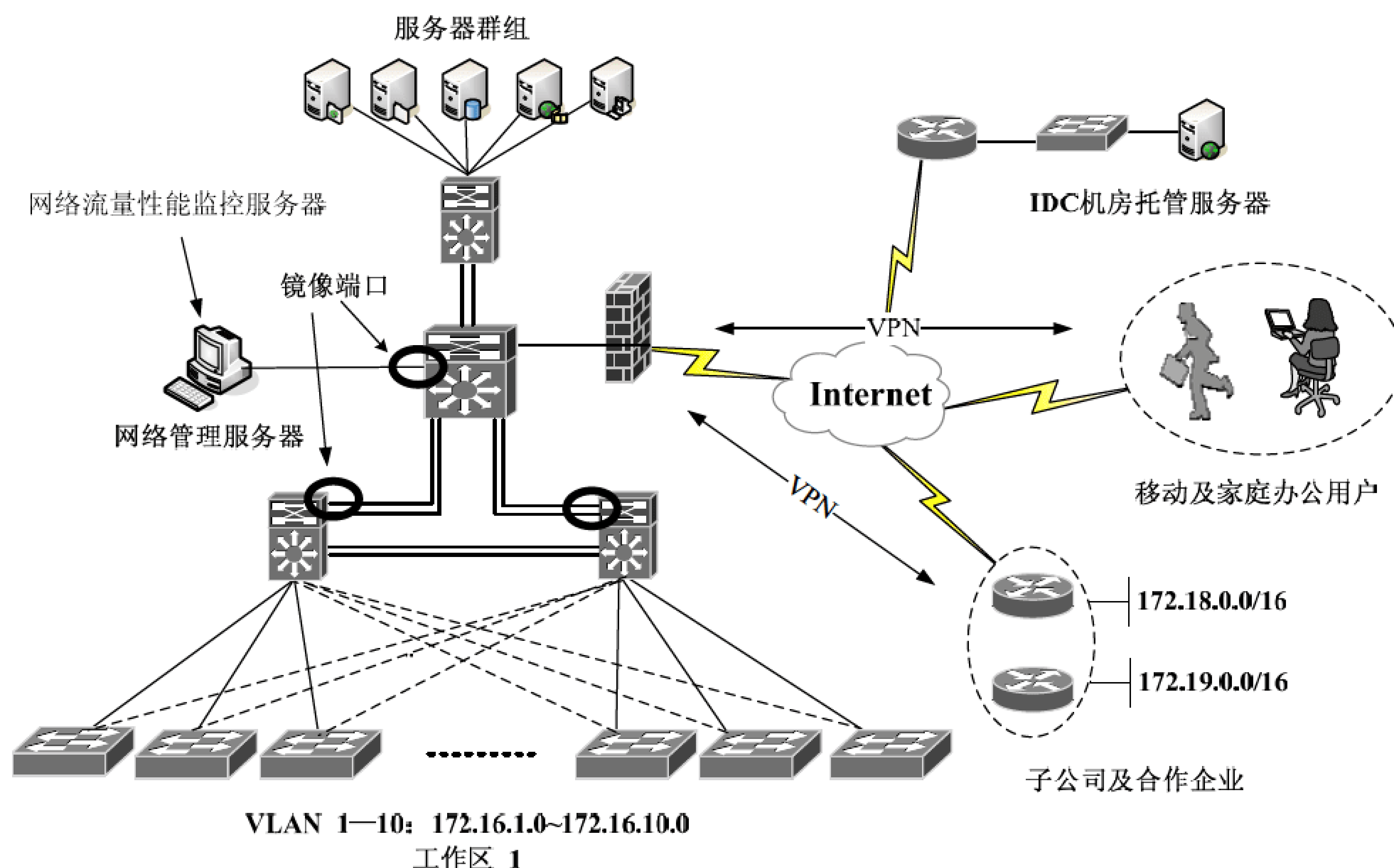


图 1-26 网络流量监测分析的拓扑图

1.3 专家答疑

（1）在网络的建设过程中，设备的调试和安装应当如何进行？

答：网络设备购买以后，厂家会有专业的技术人员提供技术调试和安装的。同时可以与对方协商设备技术培训的事宜。这样也方便了以后的维护。

（2）通过光纤传输数据时，为什么需要用两条光纤？

答：在网络数据传输过程中，都是收、发双向进行的。因此，对于光纤介质也就需要两条光纤，分别负责数据的发送和接收。虽然现在已经有了在单条光纤上同时传输收、发数据的技术，但使用双纤的场合还是占主要应用的。

（3）在网络管理实施方案执行时，应当依据什么样的基本原则？

答：网络实施方案在现实环境中执行时，要以确保网络无故障运行和数据无差错为最基本的原则。如果在执行过程中发现有不符合原则的内容，就需要及时进行协商和修改。

（4）网络信息这么多，如何从这些信息中找到有用的管理信息？

答：网络管理信息的收集要和网络管理的最终目标相结合，网络管理的目的就是掌握网络环

境状况，获知网络性能，找出网络故障隐患，使网络更稳定、更高效地运作。

除了获取网络系统配置信息外，网络性能信息也很重要，可以依靠专门网络管理工具获得。但是很多网络隐患是不能直接从性能和系统配置上看到的，如 ARP 攻击、广播风暴。这些需要网络管理员利用专业的流量监测分析工具进行操作。

流量监测分析工具可以抓获网络中的所有信息，但是真正能够构成网络威胁的可能不到一成，如何在大量的网络信息流中找出有用的流量呢？这需要管理员了解所有网络流量异常的特征。例如，如果发现网络中每秒钟的广播记录都有几百条以上，那就很有可能发生了广播风暴，又例如在流量中发现了大量数据包大小一样且小于 64 字节，可能是遭到了拒绝服务式攻击。

网络管理信息很多，作为网络管理员，一定要有耐心。

第 2 章　网络设备管理与维护基础

路由器、交换机等网络设备是网络环境中的重要组成部分，高效、合理地配置与维护这些设备对网络管理员来说显得尤为重要。本章主要介绍常用的网络设备的基础知识、配置和维护内容。

2.1　企业网络设备概述

企业中网络设备种类并不是很多，主要就是交换机和路由器。由交换机和路由器连接通信线缆，就可以构成基本的网络通信环境，所以作为网络管理员，需要熟练掌握这两种网络设备的调试配置。下面分别介绍交换机和路由器的工作原理。

1. 交换机工作原理

交换机在企业网络中主要负责局域网内客户端之间的通信，所有的客户端都通过交换机连接起来，就可以实现局域网内主机之间的资源共享和数据通信。交换机主要依靠 OSI（开放系统网络参考模型）第二层数据链路层的 MAC 地址进行寻址、数据转发。交换机还可以实现数据的差错校验、拥塞控制。

当一台主机 A 通过交换机向另一台主机 B 发送信息时，交换机获得 A 的信息后首先会查找数据包中的目标 MAC 地址，然后根据交换机本身 MAC 地址表的对应关系将信息从连接主机 B 的接口转发出去。

默认交换机连接的网络属于同一个局域网，各主机之间可以随意通信，但是为了安全，在交换机技术上提出了 VLAN 技术，即虚拟局域网技术。VLAN 技术可以将交换机连接的大的局域网划分成多个小的虚拟局域网，各个虚拟局域网之间不能直接通信，这样可以实现更好的局域网管理和安全控制。

2. 路由器工作原理

路由器的主要工作就是路径寻址、IP 数据包转发，以及拥塞控制。交换机主要负责同一个网段地址的主机互相通信，而路由器则可以实现不同网段主机间的通信，因为路由器中有路径查询的功能。

当一台主机 A 通过路由器向另一台主机 B 发送信息时，路由器获得 A 的信息后首先会查询数据包中的目标主机 IP 地址，然后和自身路由表中的条目进行比较，按照路由条目的转发规则，路由器会沿着正确的方向将数据包转发给主机 B。

路由器中的路由表相当于一个地图一样，它记录了到达指定网段的转发方向，可以很好地实现跨网段主机之间的数据通信。在互联网中使用的路由器设备比较多，而在企业网络中如果不涉及跨区域的数据通信，一般只在企业网络出口使用路由器设备。

2.2 项目实战 1：采用多种方法连接配置网络设备

在网络管理中经常会遇到调试设备的工作，应对很多的环境限制及要求，网络管理员应当灵活使用合适的设备调试方法。常见的设备调试配置的连接方法有以下几种。

2.2.1 Console 口直连配置

对网络设备进行初始化配置，或者设备无法通过网络访问时通常会使用 Console 口进行设备配置。在使用 Console 口连接配置设备时需要使用专用的设备配置线，如图 2-1 所示。配置线一般有两个接头，其中 RJ-45 接头用于连接网络设备的 Console 接口，如图 2-2 所示；另一头的 232 COM 接头用于连接计算机的 COM1 口，如图 2-3 所示。



图 2-1 设备配置线

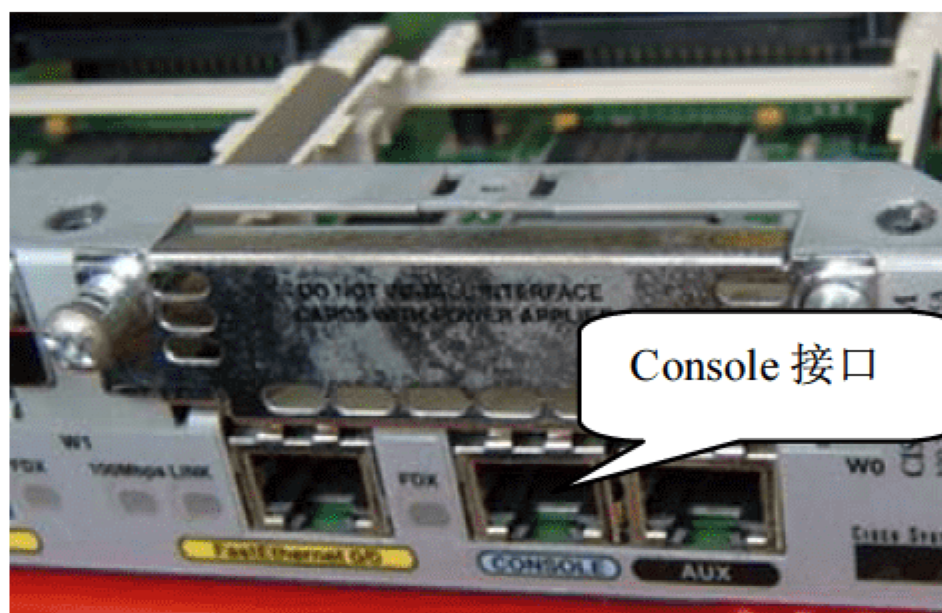


图 2-2 网络设备的 Console 接口

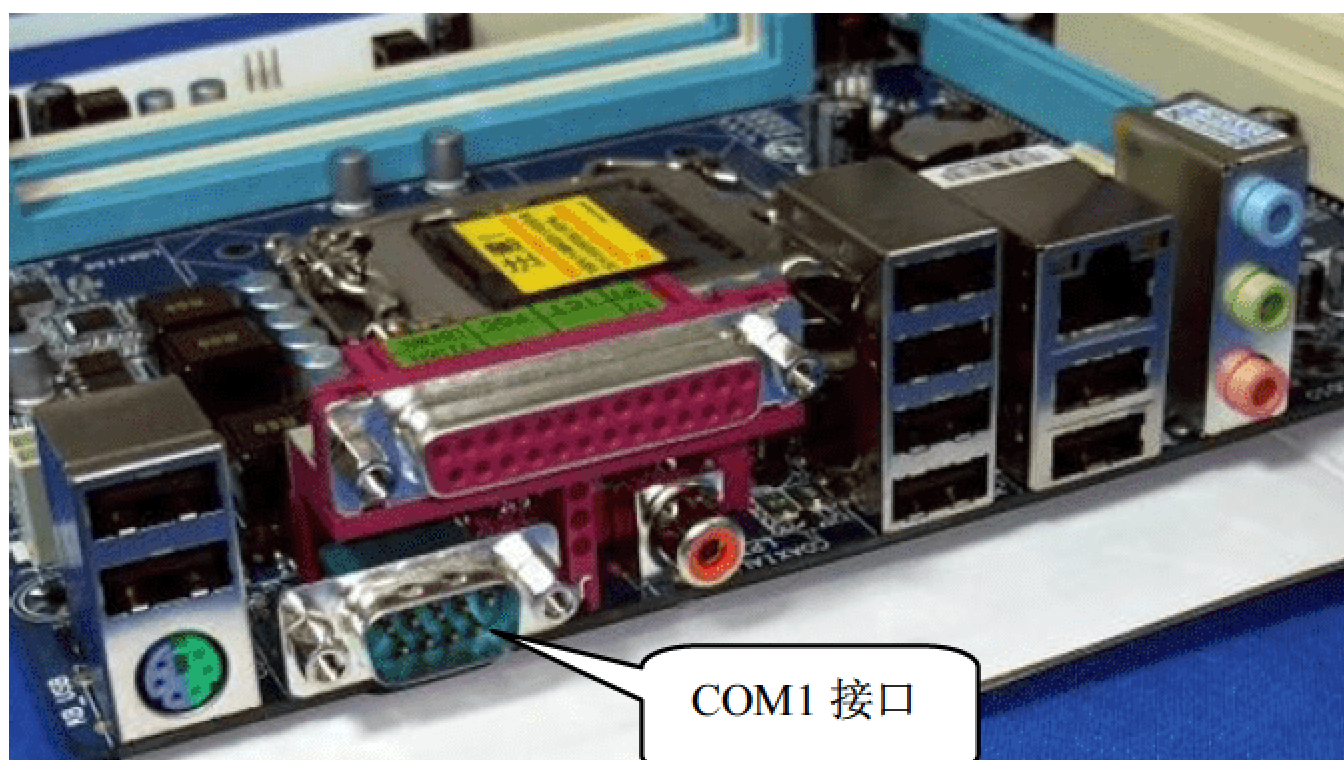


图 2-3 计算机的 COM 接口

以 Cisco 路由器为例，使用 Console 口连接配置设备的具体操作步骤如下。

01 使用 Console 线连接计算机 COM1 口与路由器的 Console 口，如图 2-4 所示。

02 在计算机中选择【开始】➢【程序】➢【附件】➢【通讯】➢【超级终端】命令，弹出

【连接描述】对话框，在【图标】选项中随意选择一个图标，并在【名称】文本框中输入本次设备连接的连接名，单击【确定】按钮，如图 2-5 所示。

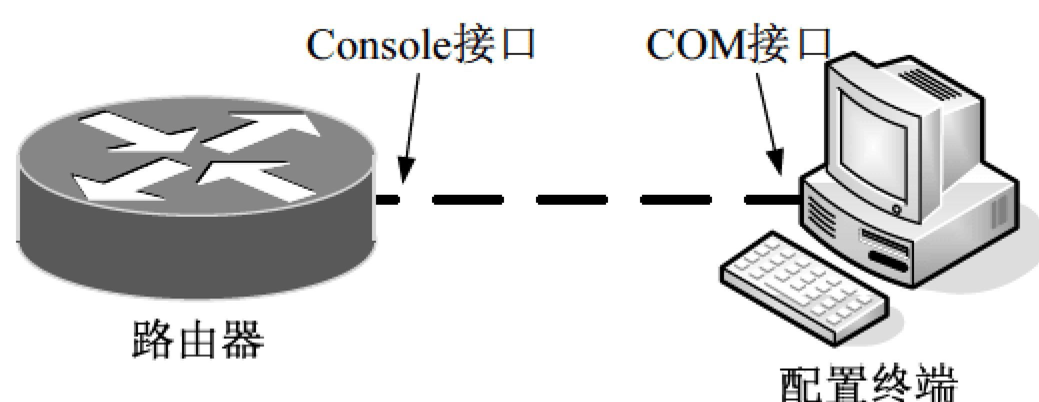


图 2-4　Console 连接拓扑图



图 2-5　【连接描述】对话框

03 弹出【连接到】对话框，在【连接时使用】下拉列表中选择【COM1】，单击【确定】按钮，如图 2-6 所示。

04 弹出【COM1 属性】对话框，显示了使用 COM1 口连接的属性。通常路由器在出厂时，传输速率为 9600bit/s，所以要为 COM1 口设置相匹配的参数，单击【还原为默认值】按钮即可。设置完成后，单击【确定】按钮，如图 2-7 所示。

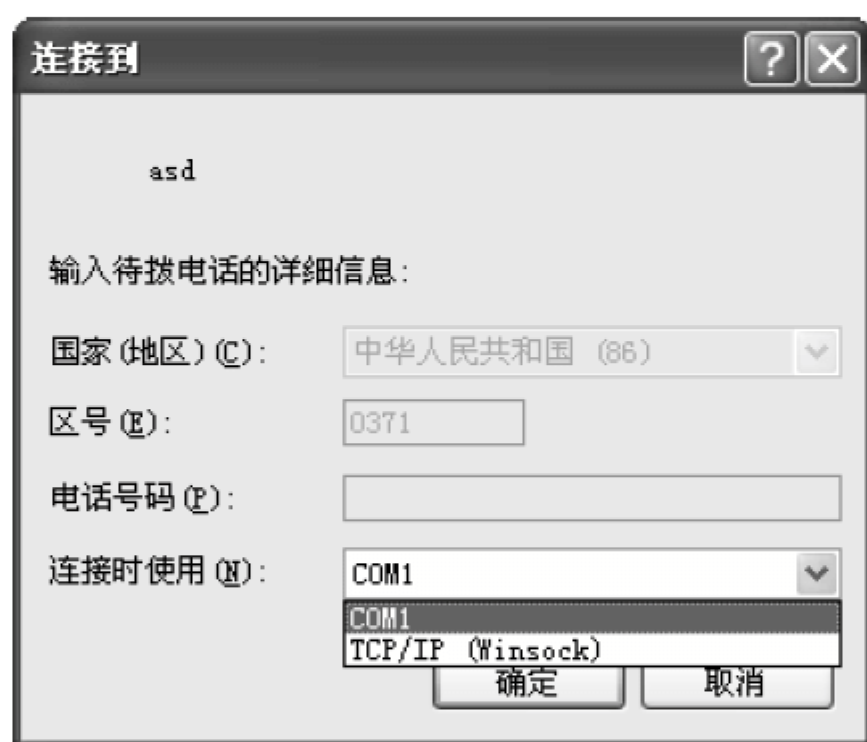


图 2-6　【连接到】对话框



图 2-7　【COM1 属性】对话框

05 开启路由器，在【超级终端】窗口中会显示路由器的开机启动信息，“#”号表示从闪存中加载 IOS 映像，如图 2-8 所示。

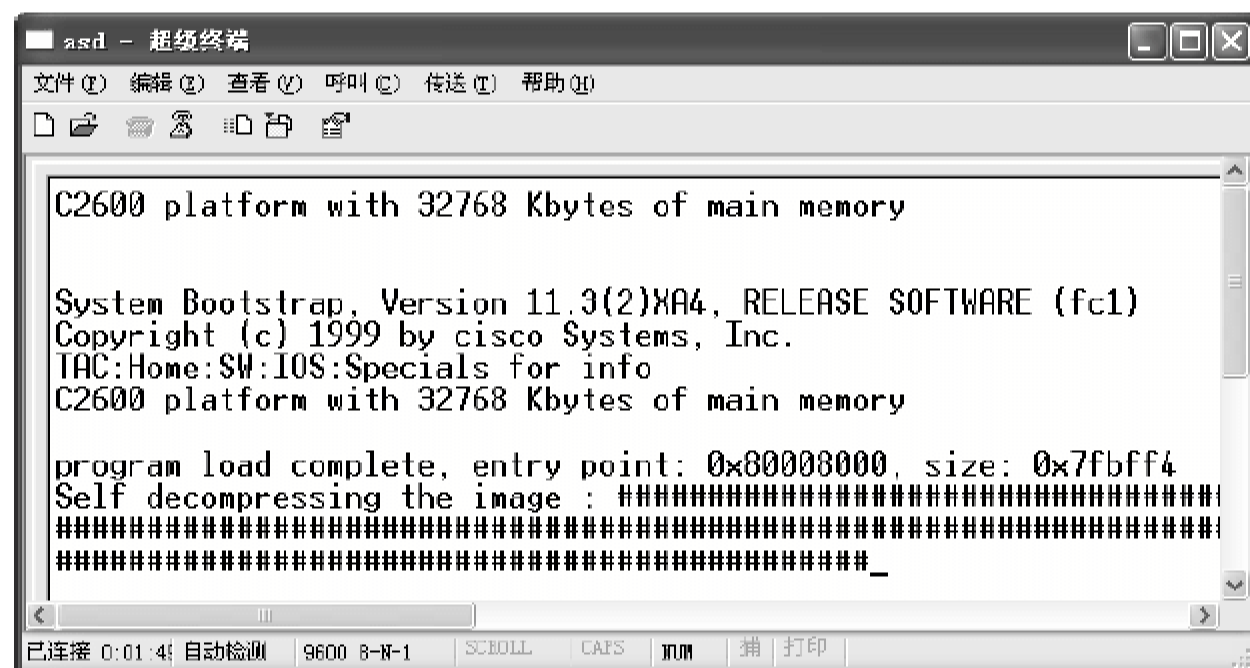


图 2-8　超级终端输出路由器启动的信息

如果超级终端无法连接到路由器，可参照以下顺序检查。

01 检查计算机和路由器之间的连接是否松动，并确保路由器已经开机。

02 在图 2-6 中，是否选择了增强的计算机 COM 口。

03 是否按照图 2-7 中设置了正确的通信参数。

04 用计算机的另一 COM 口和路由器的 Console 口连接，或者确保 COM 口正常。

05 换下 Console 线，看看结果怎样。

06 如果仍无法排除故障，而路由器非出厂设置，可能是路由器的传输速率被修改而非 9600bit/s，则逐一测试通信速率。

07 与供应商联系。

2.2.2 Telnet 远程登录配置

Telnet 远程登录配置设备是使用得比较多的一种设备配置方式，使用该方法首先要确保终端客户机能和远程设备互通，且 Telnet 流量能够通过访问控制转发。

实现设备远程登录配置的具体操作步骤如下。

01 如图 2-9 所示，模拟实验拓扑图连接网络设备。

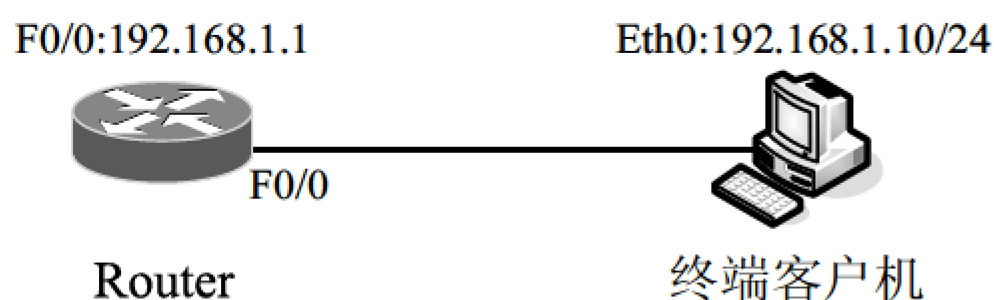


图 2-9 Telnet 实验拓扑图

02 初始化设备，并配置设备远程管理地址。

```
Router>enable
//进入特权模式
Router#configure terminal
//进入全局配置模式
Router(config)#int f0/0
//进入 F0/0 接口配置子模式
Router(config-if)#ip add 192.168.1.1 255.255.255.0
//为 F0/0 接口配置 IP 地址
Router(config-if)#no shut
//开启 F0/0 接口，默认所有路由器的接口都是 Down 状态
Router(config)#int loopback 0
//进入 loopback 0 接口配置子模式
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Router(config-if)#ip add 1.1.1.1 255.255.255.0
//为 loopback 0 接口配置 IP 地址
```


提 示

由于设备的物理接口容易损坏，所以在进行设备远程连接管理时，通常会使用 loopback 虚拟接口，该接口的 IP 地址称为设备管理地址。

03 开启设备的 Telnet 功能。

```
Router(config)#line vty 0 4
//进入虚拟接口 0-4 的配置子模式
Router(config-line)#login
% Login disabled on line 66, until 'password' is set
% Login disabled on line 67, until 'password' is set
% Login disabled on line 68, until 'password' is set
% Login disabled on line 69, until 'password' is set
% Login disabled on line 70, until 'password' is set
//开启登录功能，开启后提示允许给 5 个虚拟接口配置密码
Router(config-line)#password Cisco
//配置 VTY 口令“Cisco”
```

04 配置全局配置模式访问密码。

```
Router(config)#enable password Cisco
//配置全局配置模式的明文密码
```

或

```
Router(config)#enable secret Cisco
//配置全局配置模式的密文密码
```


提 示

远程连接设备时，必须要有全局配置模式的访问密码，否则无法配置设备。

05 配置终端客户机 IP 地址，如图 2-10 所示。

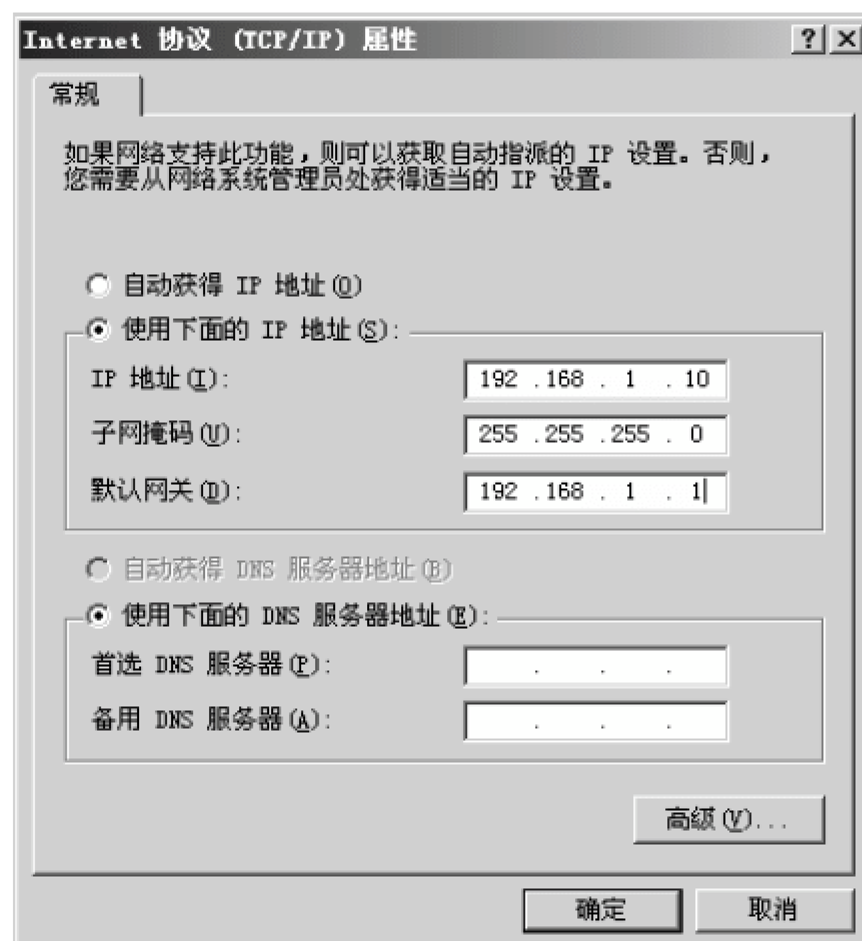


图 2-10　客户端 IP 地址配置

06 在终端客户机测试 Telnet 远程配置设备。

```
C:\Documents and Settings\Administrator>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:                    //输入密码，密码不输出显示
Router>enable
Password:
Router#
```

2.2.3 HTML 网页连接配置

使用网页连接配置设备的方式比较普遍，特别是中低端设备。使用这种方式具有直观、易操作等特征，但是在使用之前需要进行初始配置，保证终端客户机可以与被管理的设备互通，并且 Web 服务的端口允许转发。

可以使用网页连接配置的设备在出厂时大都会配置设备管理地址，以及访问账户与密码，使用得较多的设备管理地址为“192.168.1.1”或“192.168.0.1”。

2.3 构建路由交换模拟实验环境

在学习过程中，读者不一定能接触到真实的网络设备，即便是已经从事网络管理或网络工程建设的工作者，由于刚刚入行，也很少有机会接触高端的网络设备，所以在学习路由交换技术时往往需要借助模拟器设备。本节主要介绍比较流行的模拟器软件 DynamipsGUI，具体内容如下。

思科路由模拟器 Dynamips 与思科官方的 Cisco Packet Tracer 模拟器相比，具有更真实的实验环境，它消耗计算机系统资源来模拟实验环境，硬件配置决定了能够模拟出的实验环境规模。使用 Dynamips 模拟器像操作真实网络设备一样，可以锻炼读者的实际设备操作能力。Dynamips 安装程序目录中主要包括一个 IOS 目录和两个执行文件，如图 2-11 所示。



图 2-11　Dynamips 安装程序目录

IOS 文件夹内存放了真实的 Cisco IOS 系统，模拟实验时可以根据需求选择合适的 IOS 系统，选择比较灵活，如图 2-12 所示。

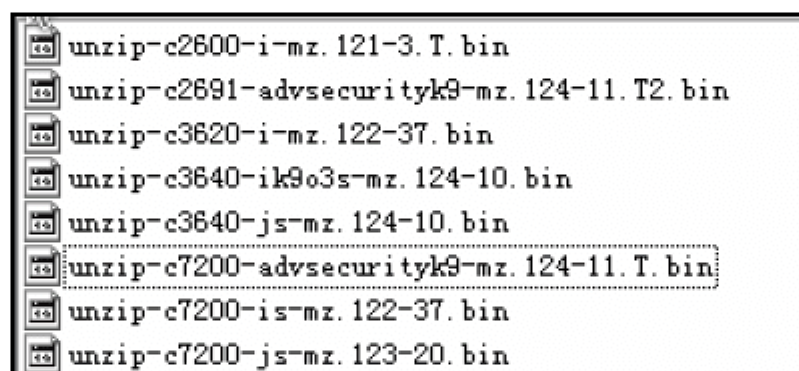


图 2-12　Dynamips 默认的 IOS 系统

2.3.1　安装 DynamipsGUI 模拟器

在正式安装主程序之前，先要安装好 WinPcap 网络驱动包，否则网络模拟器软件将无法正常安装。具体操作步骤如下。

01 双击安装目录下的 WinPcap 程序包，弹出 WinPcap 安装向导欢迎对话框，单击【Next】按钮，如图 2-13 所示。

02 弹出【License Agreement】对话框，单击 I Agree 按钮，如图 2-14 所示。

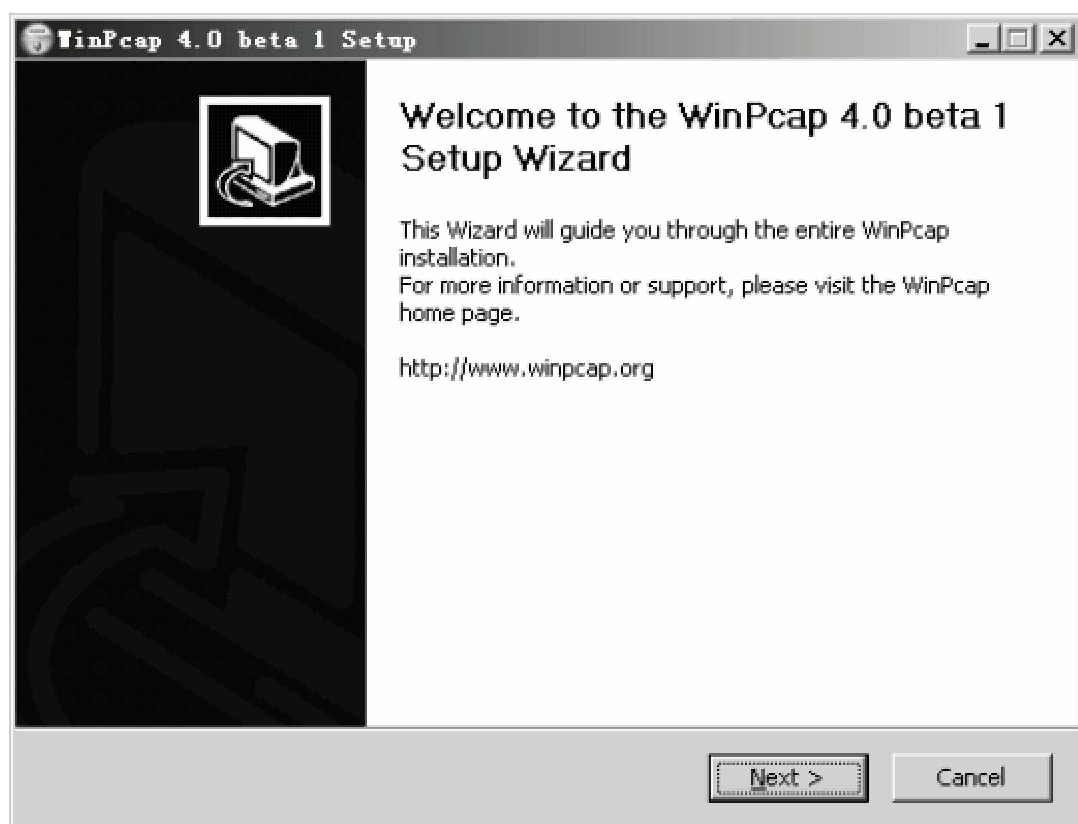


图 2-13　WinPcap 安装向导欢迎对话框

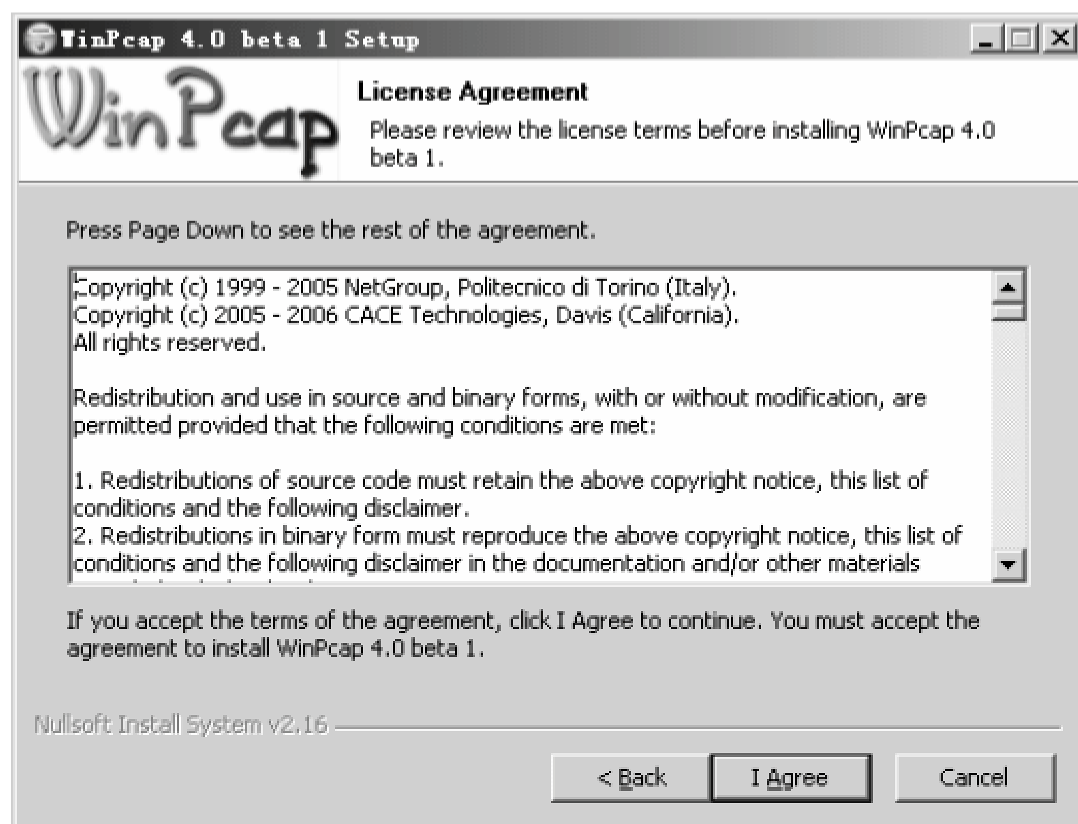


图 2-14　【License Agreement】对话框

03 弹出【Installing】对话框，并显示安装进度，如图 2-15 所示。

04 安装完成，弹出完成安装向导对话框，单击【Finish】按钮，如图 2-16 所示。

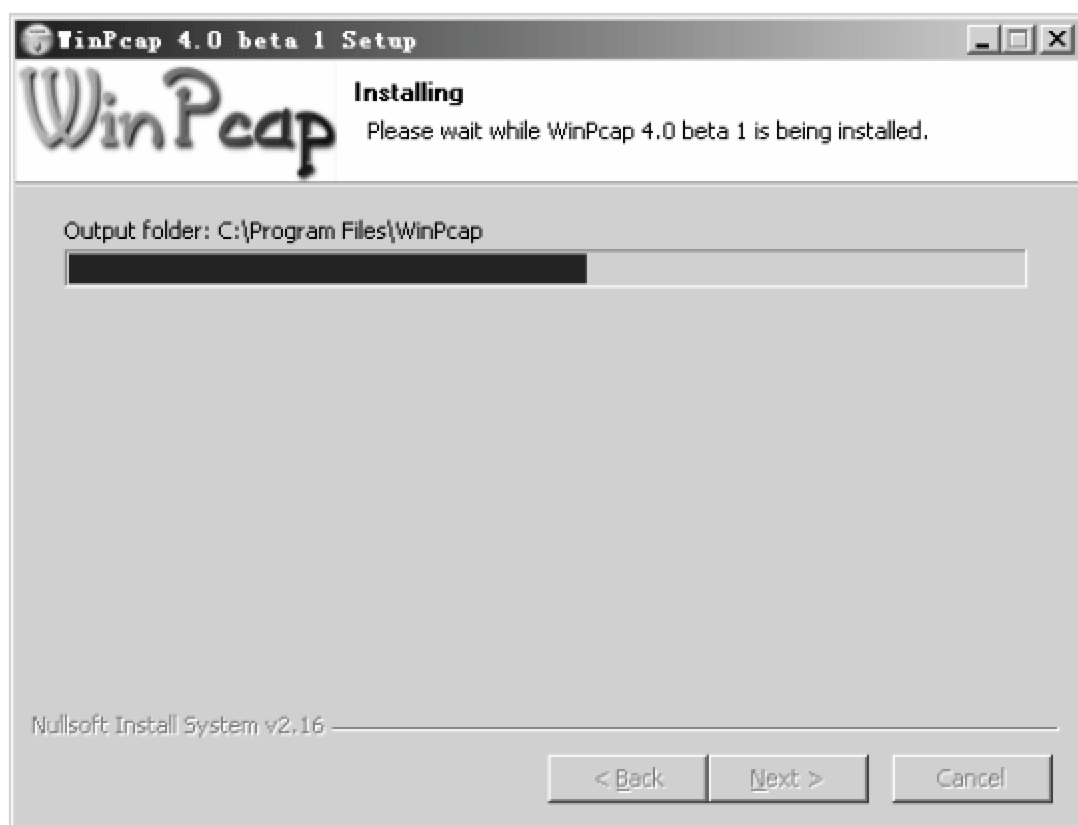


图 2-15　【Installing】对话框

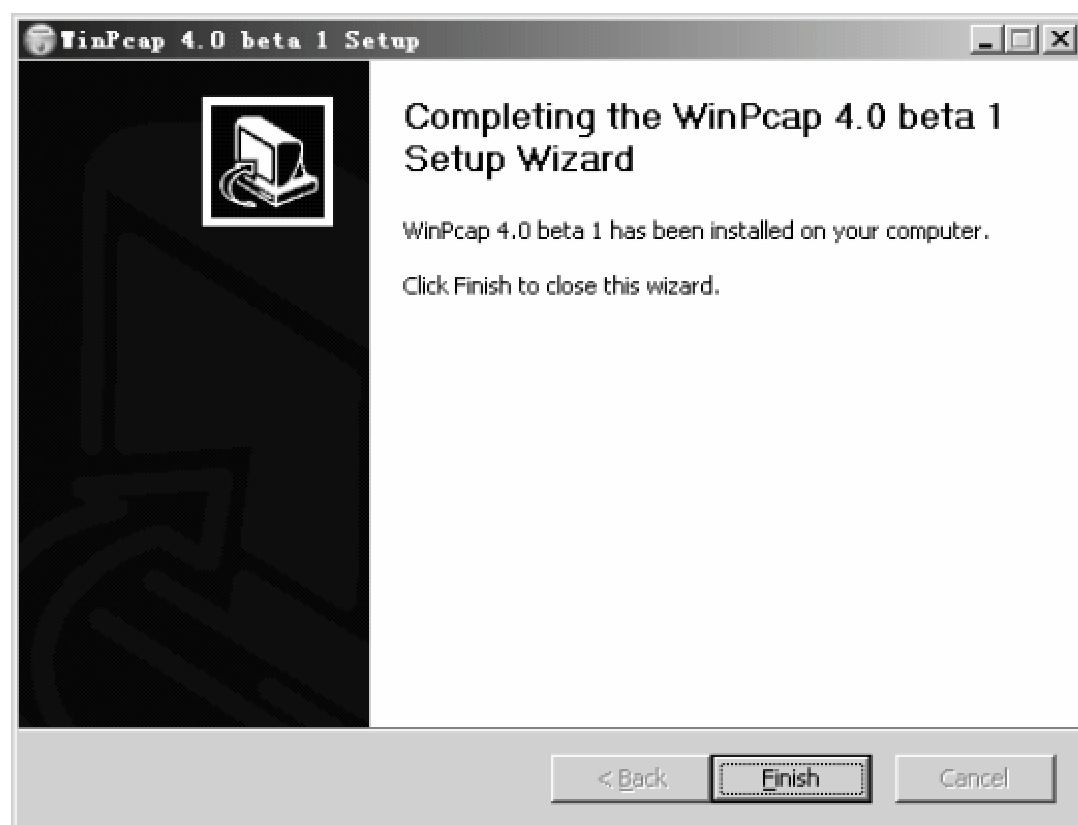


图 2-16　完成安装向导对话框

05 双击 DynamipsGUI 安装程序，弹出【欢迎】对话框，单击【下一步】按钮，如图 2-17 所示。

06 弹出【许可协议】对话框，选中【我同意该许可协议的条款】单选按钮，单击【下一步】按钮，如图 2-18 所示。

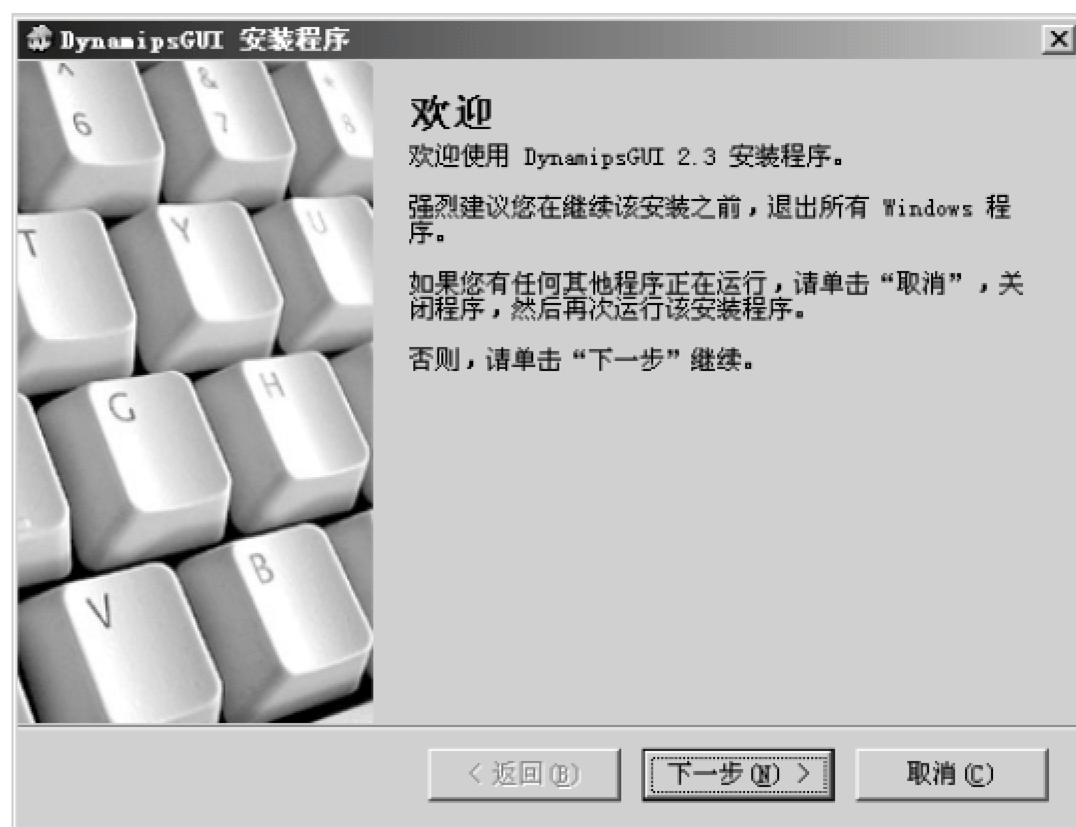


图 2-17 【欢迎】对话框



图 2-18 【许可协议】对话框

07 弹出【用户信息】对话框，在【名称】和【公司】文本框中分别输入读者身份信息，单击【下一步】按钮，如图 2-19 所示。

08 弹出【安装文件夹】对话框，指定程序的安装目录，单击【下一步】按钮，如图 2-20 所示。



图 2-19 【用户信息】对话框



图 2-20 【安装文件夹】对话框

09 弹出【快捷方式文件夹】对话框，指定安装后桌面产生的快捷方式名，采用默认配置，单击【下一步】按钮，如图 2-21 所示。

10 弹出【准备安装】对话框，显示安装配置信息，单击【下一步】按钮，如图 2-22 所示。

11 弹出【正在安装 DynamipsGUI】对话框，显示安装进度，如图 2-23 所示。

12 安装完成，弹出【安装成功】对话框，单击【完成】按钮，如图 2-24 所示。

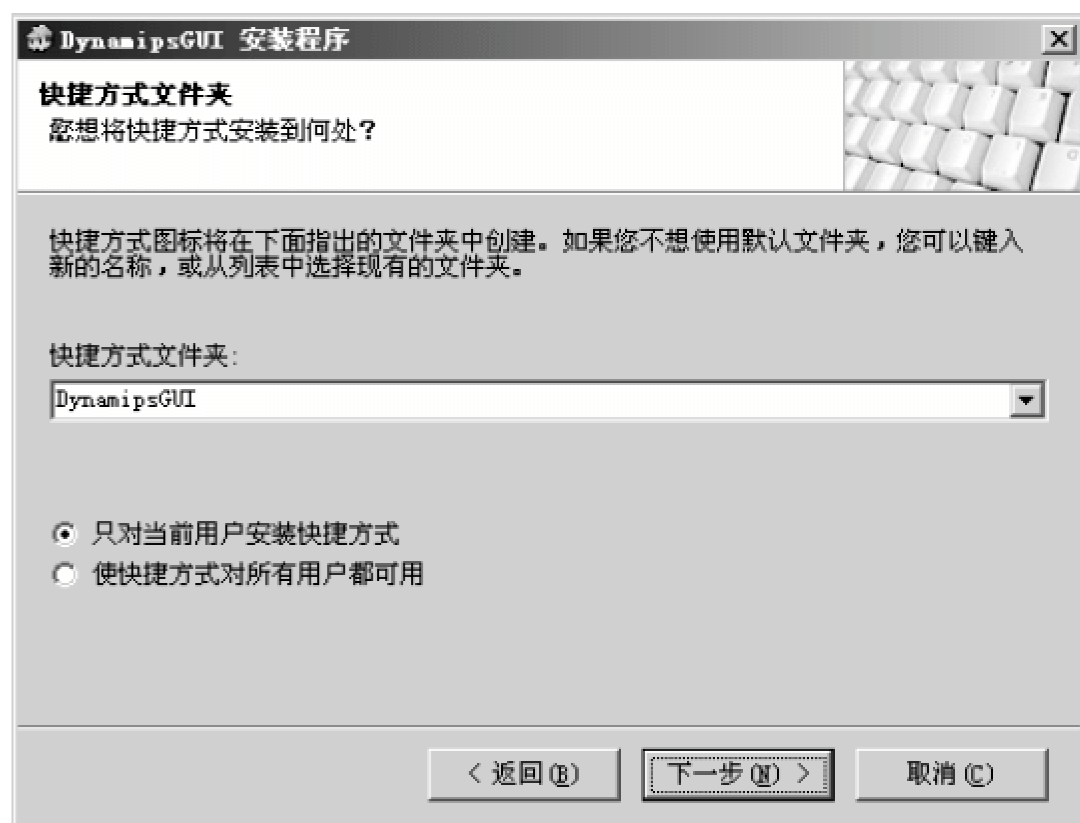


图 2-21　【快捷方式文件夹】对话框

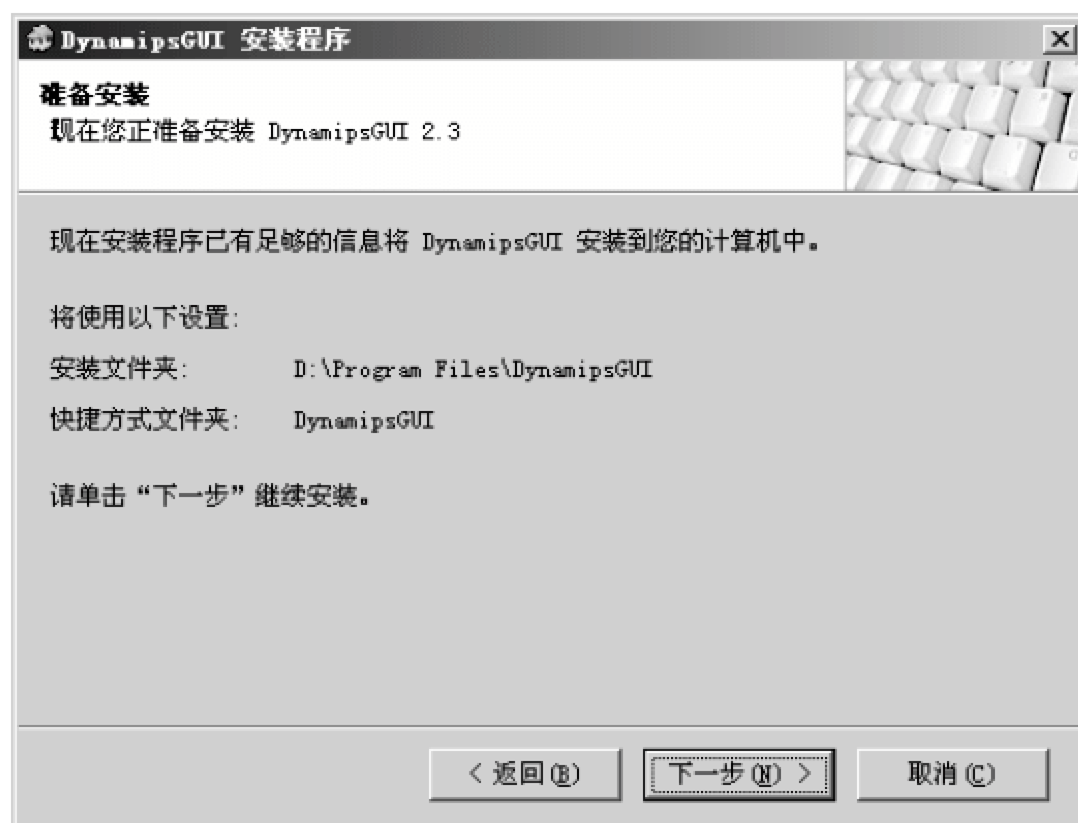


图 2-22　【准备安装】对话框

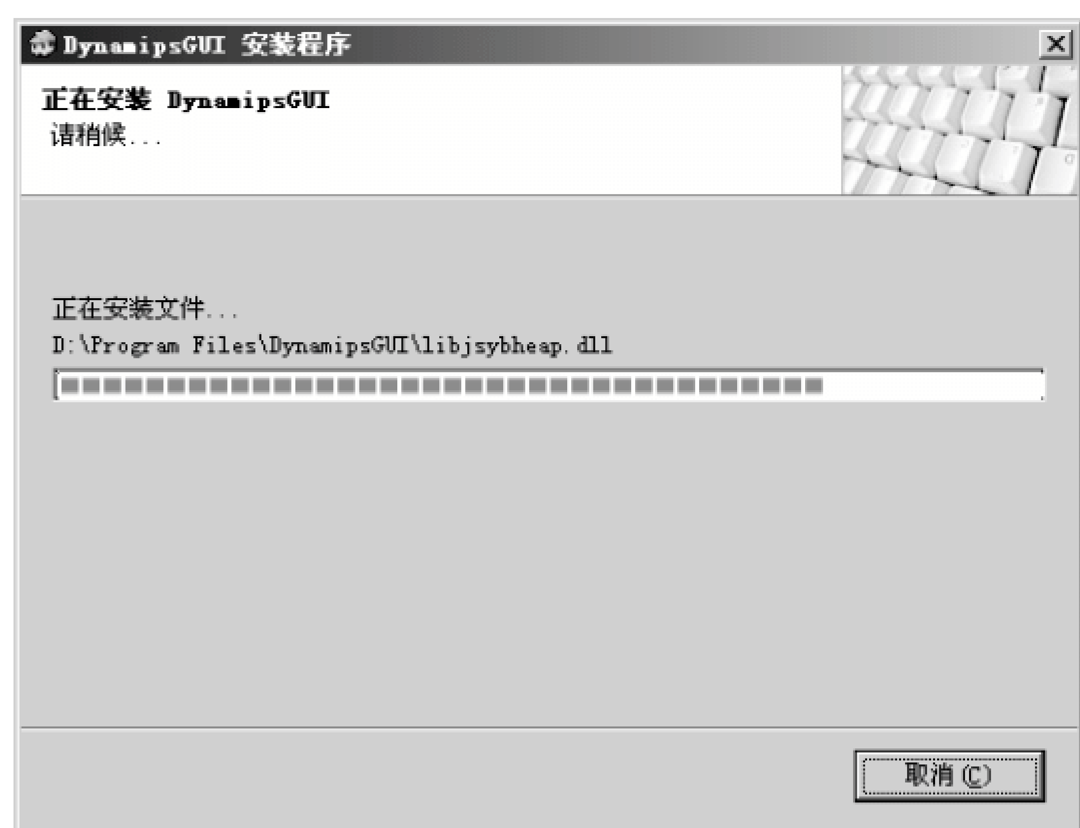


图 2-23　【正在安装 DynamipsGUI】对话框



图 2-24　【安装成功】对话框

2.3.2　使用 DynamipsGUI 模拟器

安装完毕，桌面上会出现 DynamipsGUI 的快捷方式。虽然 DynamipsGUI 模拟器使用效果比较好，但是在进行模拟实验之前必须要进行烦琐的配置，具体操作步骤如下。

01 双击运行 DynamipsGUI 程序，打开程序的主界面，程序主界面包括 6 个区域，要进行分别配置，如图 2-25 所示。首先在①区【路由器个数】下拉列表中指定模拟环境要使用的路由设备个数，并选中【桥接到 PC】复选框指定要模拟的硬件环境。

02 在图 2-25 所示界面的②区选择合适的设备型号，并不是型号越高越好，建议选择 3640 系列的产品型号。在③区为每一个设备类型指定 IOS 系统文件，单击【浏览】按钮，可以在程序安装目录下的 IOS 目录找到合适的 IOS 系统文件，要在【idle-pc 值】文本框输入合适的 CPU 压力值则单击【计算 idle】按钮，如图 2-26 所示。

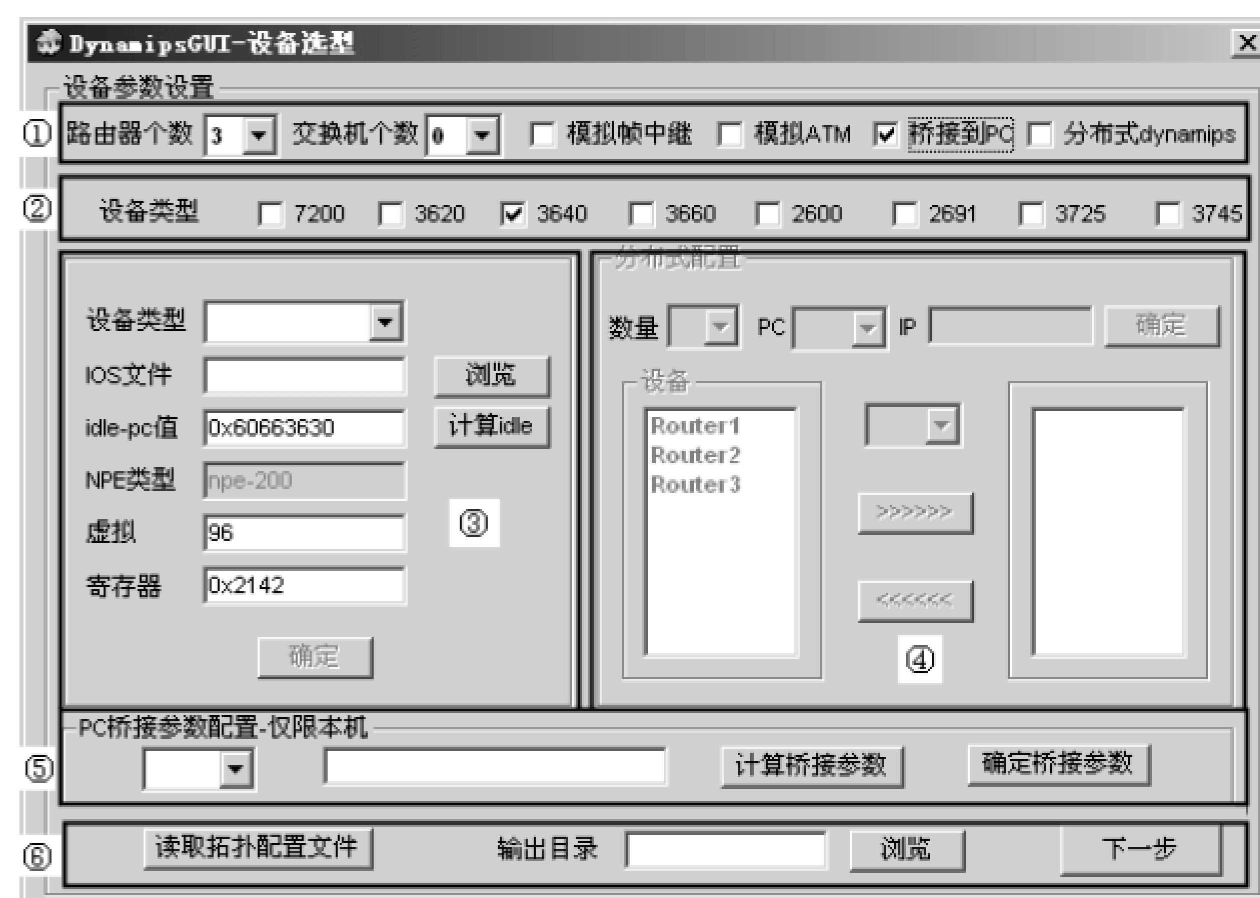


图 2-25　Dynamips 程序的主界面



图 2-26　指定设备类型的相关配置

03 弹出命令行界面，按任意键启动路由器设备，如图 2-27 所示，输入 n。

```
Cisco 3640 (R4700) processor (revision 0xFF) with 94208K/4096K bytes of memory.
Processor board ID 00000000
R4700 CPU at 100MHz, Implementation 33, Rev 1.2
DRAM configuration is 64 bits wide with parity enabled.
125K bytes of NVRAM.
8192K bytes of processor board System flash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: _
```

图 2-27　启动路由器设备

04 初始化路由器，进入路由器的用户登录模式，随意输入以下字符，然后按 Ctrl+]组合键，松开后迅速按下 i 键，如图 2-28 所示。

```
Cisco IOS Software, 3600 Software (C3640-IK9O3S-M), Version 12.4(10), RELEASE SO
FTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 16-Aug-06 04:04 by prod_rel_team
*Mar  1 00:01:04.871: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
 a cold start
Router>
```

图 2-28　进入路由器的用户登录模式

05 路由器经过一段时间的运算，计算出可用的 idle 值，一般选择使用最大值会有较好的 CPU 使用效果，但实际上最大不一定最好，建议选择排名第二或第三的值，如图 2-29 中的值“0x605c9218 (count=60)”。

```
Router>ii
Please wait while gathering statistics...
Done. Suggested idling PC:
   0x605c88d4 (count=48)
   0x605c8904 (count=37)
   0x605c8ad0 (count=43)
   0x605c8b40 (count=43)
   0x605c9218 (count=60)
   0x60559578 (count=22)
   0x605c9598 (count=20)
   0x605c95b4 (count=29)
   0x605c95f4 (count=80)
   0x604a9904 (count=36)
Restart the emulator with "--idle-pc=0x605c88d4" (for example)
```

图 2-29　计算出可用的 idle 值

06 返回程序主界面，在【idle-pc 值】文本框中输入计算出的值，【虚拟】文本框表示使用的内存量，采用默认配置，【寄存器】文本框输入的是路由器重启后设备的寄存器值，值 0x2142 表示启动设备时不加载 startup-config 配置文件，一般要将此值改为 0x2102，使设备启动时可以加载配置文件，如图 2-30 所示。



图 2-30　Dynamips 程序主界面

07 ④区是一种 Dynamips 的分布式应用，一般不使用，在⑤区可以配置物理设备和虚拟环境的桥接，使虚拟环境和真实环境联系在一起，一般选择【NIC-0】接口连接，单击【计算桥接参数】按钮，如图 2-31 所示。



图 2-31　PC 桥接参数配置

08 弹出命令行界面，给出了可桥接的网卡信息，要选择本地的物理网卡信息，如图 2-32 所示。

```
Network device list:

   rpcap://\Device\NPF_GenericDialupAdapter : Network adapter 'Adapter for gener
ic dialup and VPN capture' on local host
   rpcap://\Device\NPF_{6E232745-3171-4810-93FE-5A13A3B1FD9A} : Network adapter
'Realtek 10/100/1000 Ethernet NIC                          (Microsoft's P
acket Scheduler) ' on local host

 软件支持单/双网卡桥接，你可以选择使用任何一种
 请复制你要桥接的网卡参数，返回主界面后依次填入你要桥接的网卡
 例\Device\NPF_{2CD5187F-2A2A-4AF9-8009-531D37B51B3B}
请按任意键继续. . .
```

图 2-32　获取桥接网卡信息

09 将找到的网卡信息复制到文本框中，单击【确定桥接参数】按钮，如图 2-33 所示。



图 2-33　录入桥接网卡信息

10 在⑥区【输出目录】文本框中输入该模拟环境文件的保存位置，输入完成后单击【下一步】按钮，如图 2-34 所示。



图 2-34　指定输入目录

11 弹出【详细信息设置】界面，在左侧列表中分别选择设备，在【设备名称】文本框中指定设备名，在【设备类型】下拉列表中指定该设备类型，【Console 口】文本框的值是 Telnet 连接该设备的端口，在【模块设置】区域为设备指定要使用的接口模块，例如【Slot1】下拉列表中的值 “NM-4E” 表示有 4 个以太网接口的模块,当一个设备的配置设定好之后要单击【确定（*）配置】按钮。所有的设置配置完毕，单击【下一步】按钮，如图 2-35 所示。



图 2-35　【详细信息设置】界面

12 弹出提示框，一旦确认将无法修改之前的配置，单击【确定】按钮，如图 2-36 所示。

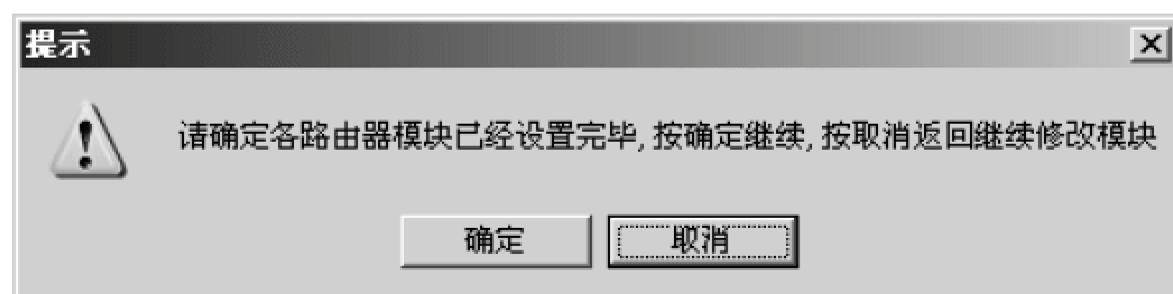


图 2-36　配置确认提示框

13 弹出【Dynamips 连接设置】对话框，左右两侧分别选择要连接的设备，以及进行连接的接口，单击【连接】按钮，弹出连接成功提示框。依次将需要连接的接口进行连接，在【连接信息】

窗格中显示了连接信息，建议将连接信息保存，方便以后查看。连接完所有设备接口后单击【生成BAT 文件】按钮，如图 2-37 所示。



图 2-37 连接设备接口

14 弹出提示对话框，一旦确认接口连接配置将不可修改，单击【确定】按钮，如图 2-38 所示。

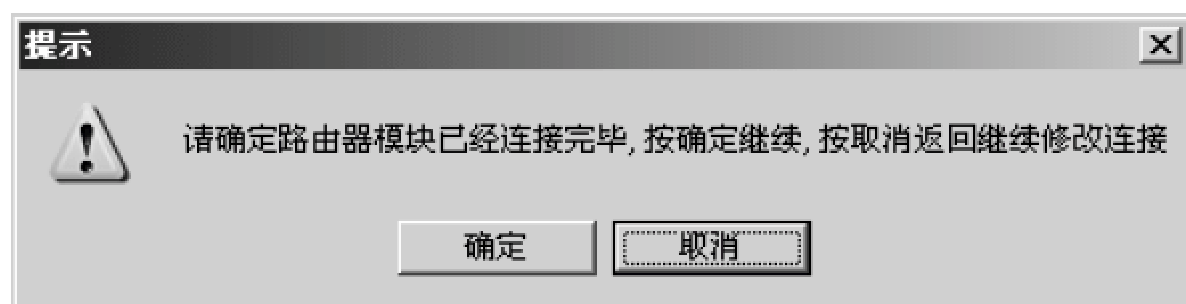


图 2-38 确认提示对话框

15 弹出命令行界面，显示生成文件，全部生成后按任意键，如图 2-39 所示。

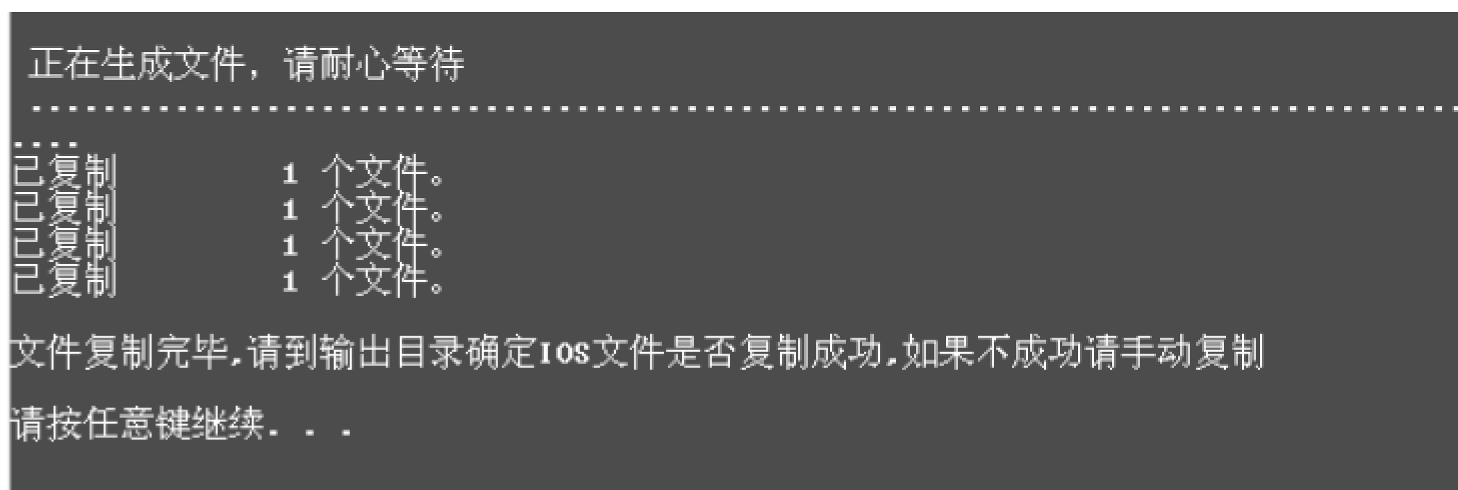


图 2-39 生成文件

16 生成文件完毕弹出提示框，单击【确定】按钮，如图 2-40 所示。



图 2-40 生成文件完毕提示框

17 打开曾配置的输出目录，打开“pc1”文件夹，可以看到搭建虚拟环境所产生的多个文件，3 个 Router*.bat 文件就是创建的 3 个路由器设备文件，双击运行 Router1.bat 文件，如图 2-41 所示。



图 2-41 生成的模拟环境文件

18 弹出该路由器启动后的命令行界面，如图 2-42 所示，将该窗口最小化。

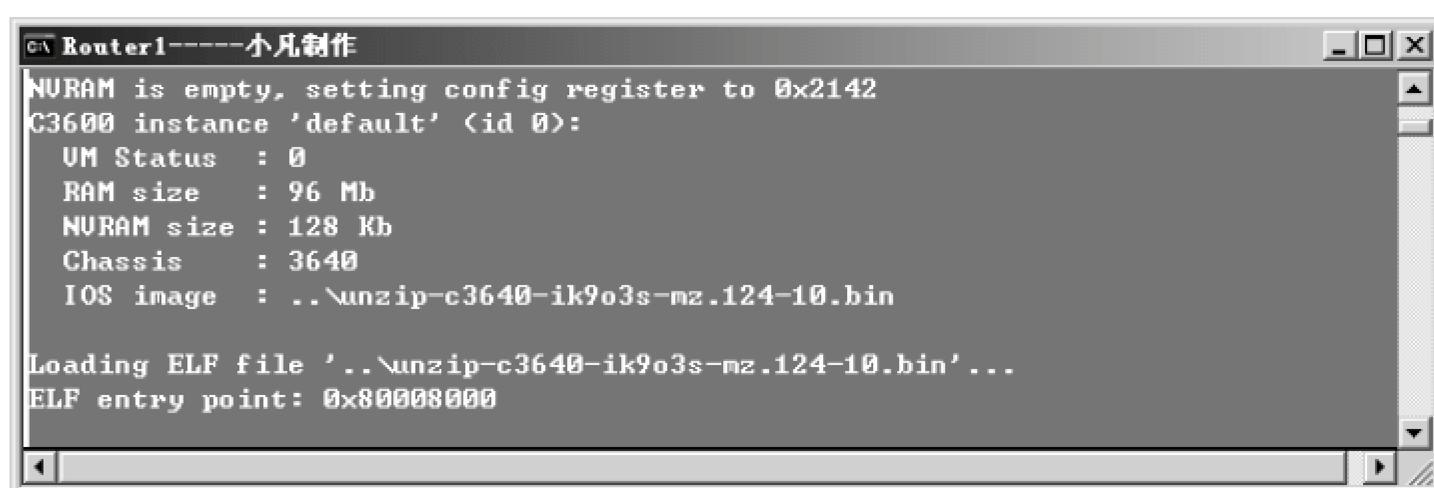


图 2-42 运行路由器启动文件

19 在本机打开命令行界面，输入“telnet 127.0.0.1 2001”命令，即可登录 Router1 路由器，如图 2-43 所示。



图 2-43 连接配置好的模拟路由器

通过以上方法连接所有设备后，就可以根据需求进行配置了。从以上配置可以看出，在使用 Dynamips 模拟器时必须保证网络拓扑图的准确性，一旦搭建好模拟环境将无法修改。

2.4 网络设备常用配置案例

网络设备作为网络环境中的重要组成部分，网络管理员必须要熟悉其操作。下面主要介绍常见的网络设备操作案例。

2.4.1　项目实战 2：备份与恢复设备配置文件

网络设备作为固件，难免会出现故障，如果设备坏了则更换一个新设备就行了。但是整个网络的运作不是拥有完好的设备就可以实现的，更需要设备系统及合理的配置，所以对于设备来说，最重要的不是设备硬件本身，而是其中的配置文件。

以 Cisco 设备为例，配置文件主要有“running-config”和“startup-config”两个，其中“startup-config”是可存储的配置文件，也是主要用于备份的配置文件。

当设备配置结束，整个网络可以正常运作时，网络管理员应当将关键设备的配置文件进行备份。一旦设备出现故障，要能够在第一时间修复设备硬件并将之前备份的配置文件进行恢复。

下面详细介绍设备配置文件备份与恢复的操作方法。

1. 实验拓扑

首先，在实现设备配置文件备份时需要使用 TFTP 服务器。TFTP 服务器与网络设备之间不一定直连，本实例采用如图 2-9 所示的网络拓扑图进行介绍。

2. 搭建 TFTP 服务器

TFTP 软件有很多种，本实例选择 Cisco TFTP Server，该软件可以免费获得。在 TFTP 服务器上安装 Cisco TFTP Server 软件，具体操作步骤如下。

01 运行 Cisco TFTP Server 安装程序，弹出【Welcome】对话框，单击【Next】按钮，如图 2-45 所示。

02 弹出【Choose Destination Location】对话框，单击【Browse】按钮可以修改 TFTP 程序的安装目录，本实例采用默认配置，单击【Next】按钮，如图 2-45 所示。

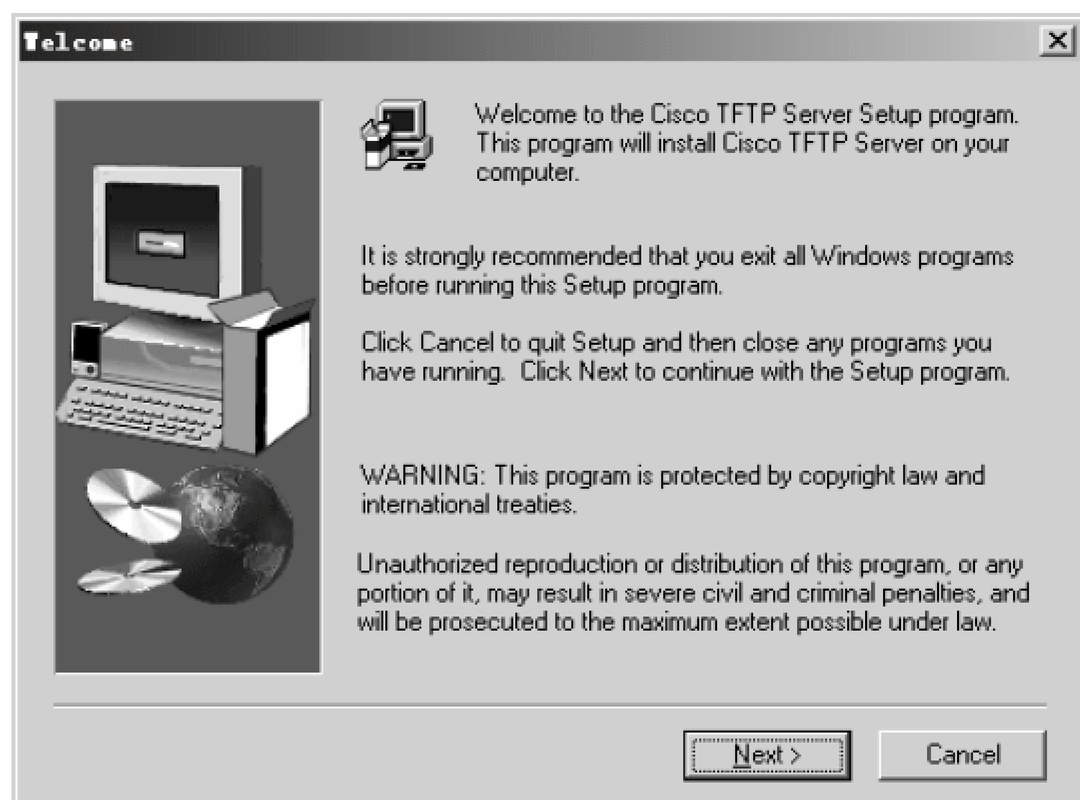


图 2-44　【Welcome】对话框

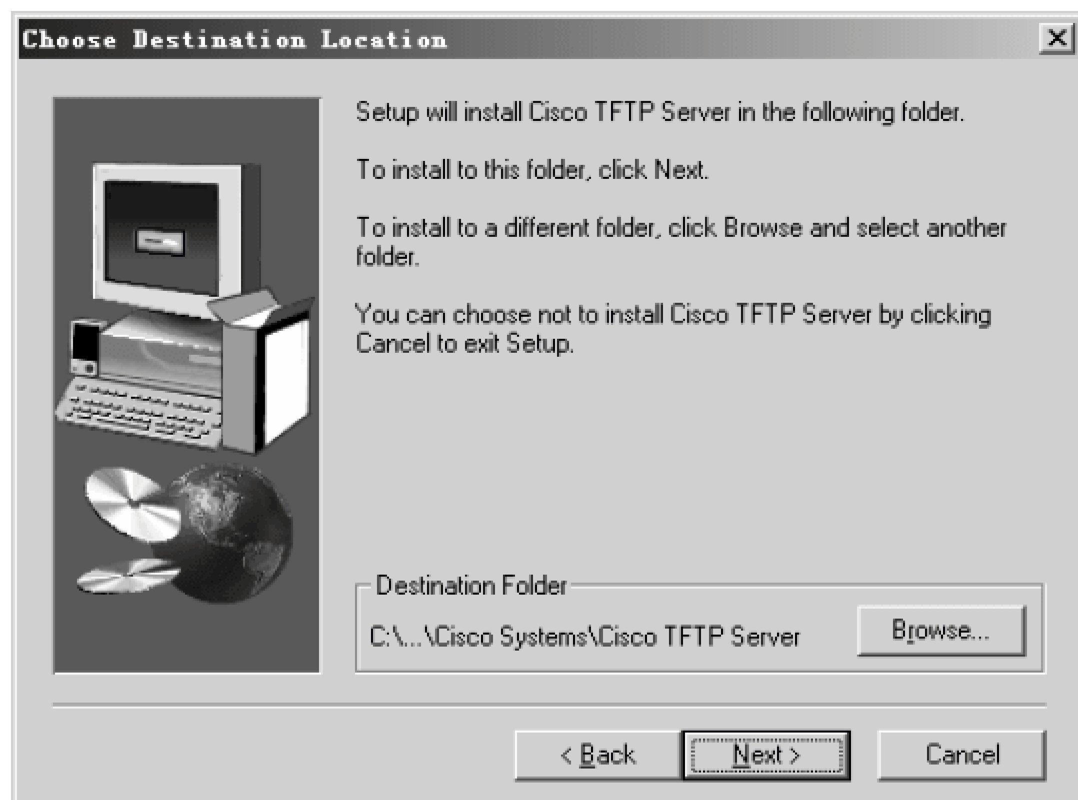


图 2-45　【Choose Destination Location】对话框

03 弹出【Select Program Folder】（选择程序文件夹）对话框，采用默认配置，单击【Next】按钮，如图 2-46 所示。

04 弹出【Setup Complete】对话框，单击【Finish】按钮，如图 2-47 所示。

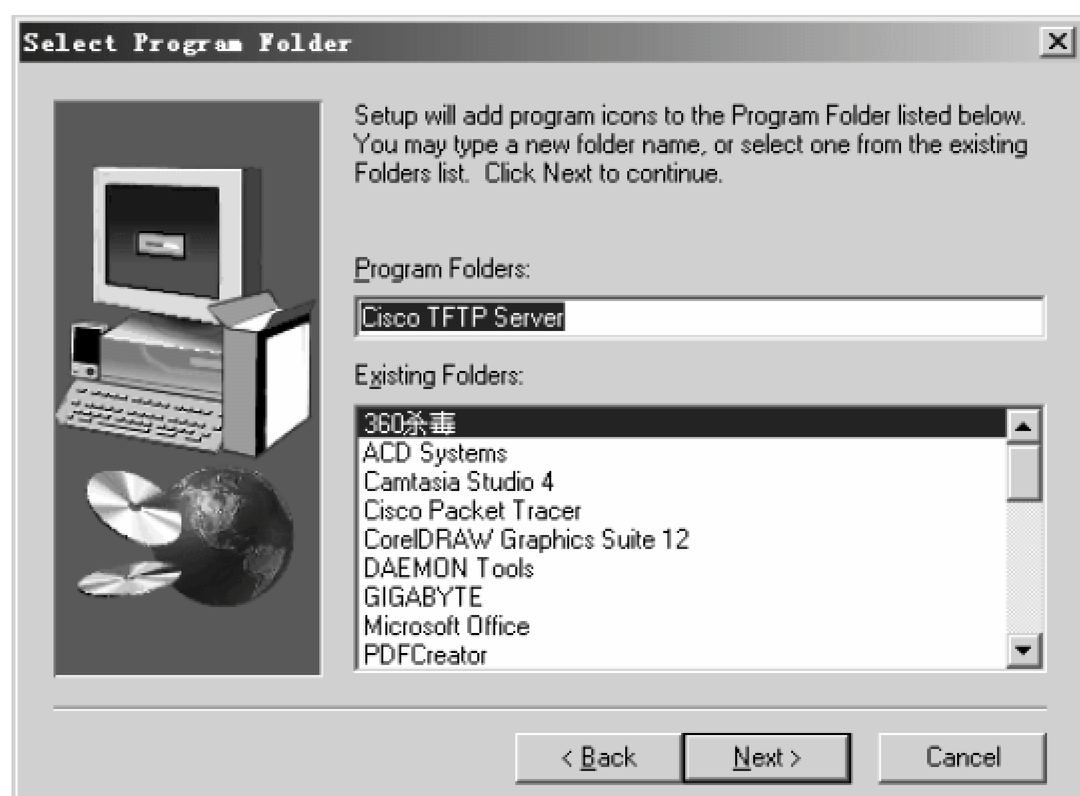


图 2-46 【Select Program Folder】对话框

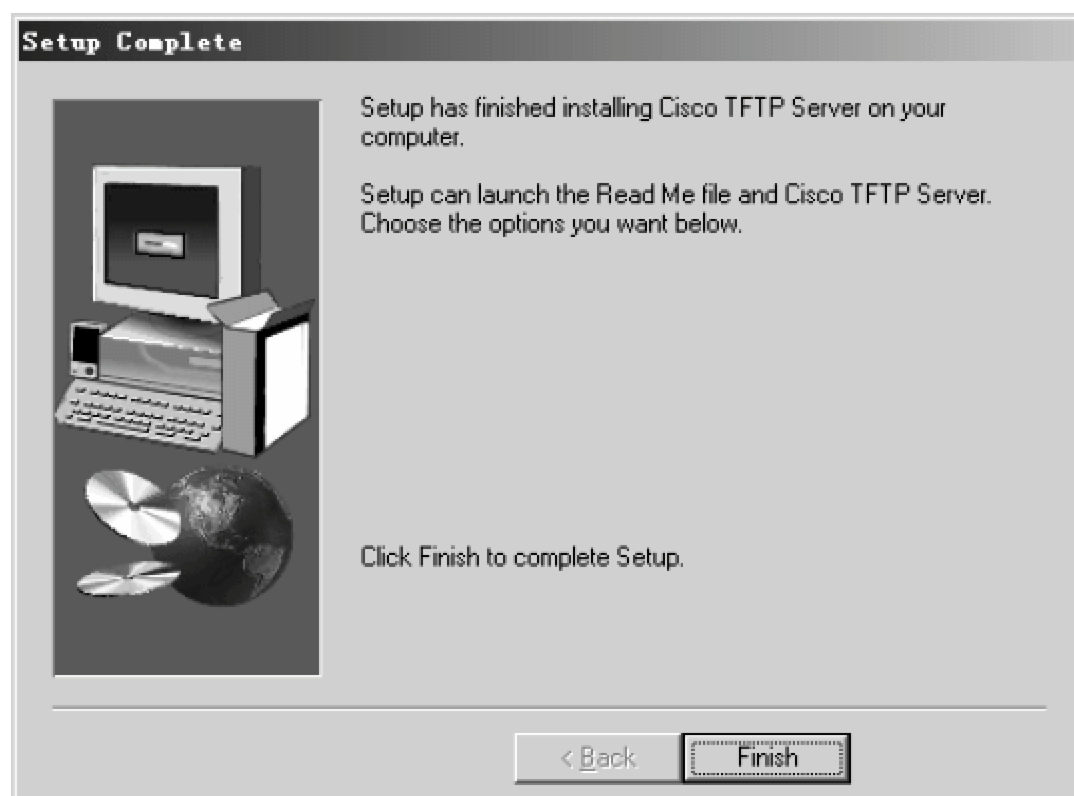


图 2-47 【Setup Complete】对话框

05 安装完成后会在桌面显示 TFTP 程序的快捷方式图标。双击程序图标，打开程序窗口，选择菜单栏【View】➢【Options】命令，如图 2-48 所示。

06 弹出【Options】对话框，可以对 TFTP 服务器进行配置。【Log】（日志）文本框用于指明程序日志文件的目录；【Maximum log file size】（最大日志文件大小）用于限制日志文件的大小，一旦超出限定值会自动删除过期日志；【TFTP server root】显示了 TFTP 服务器的根目录，通过 TFTP 服务器保存的文件会自动的存储在根目录下。本实例全部采用默认配置，单击【OK】按钮，如图 2-49 所示。

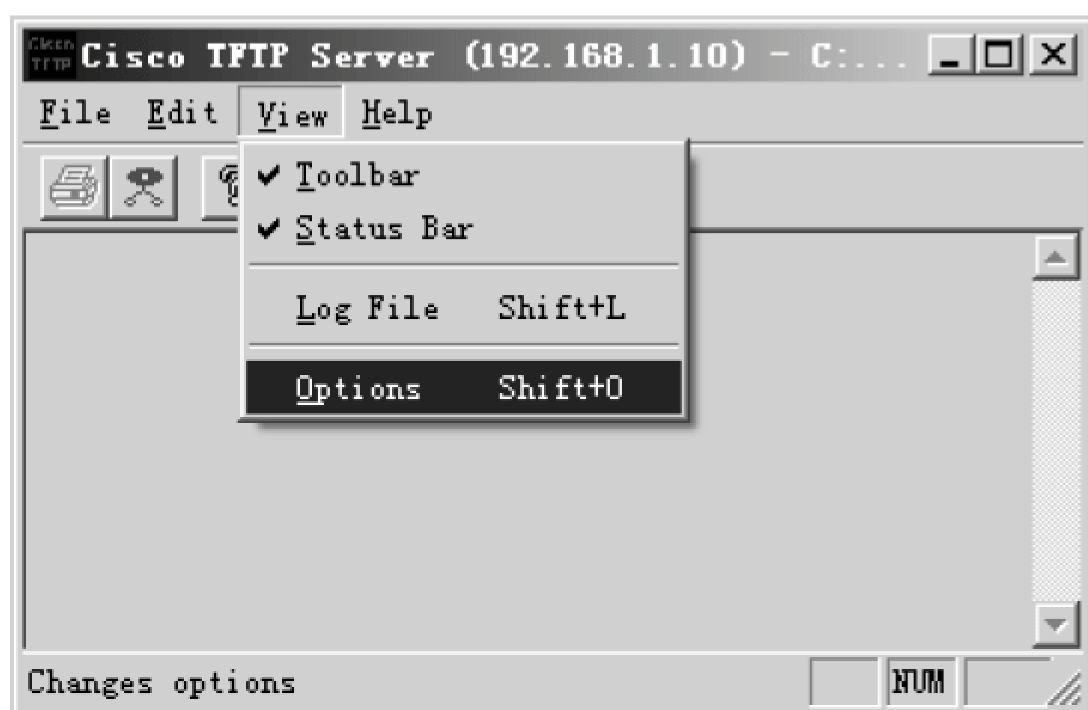


图 2-48 Cisco TFTP Server 主界面

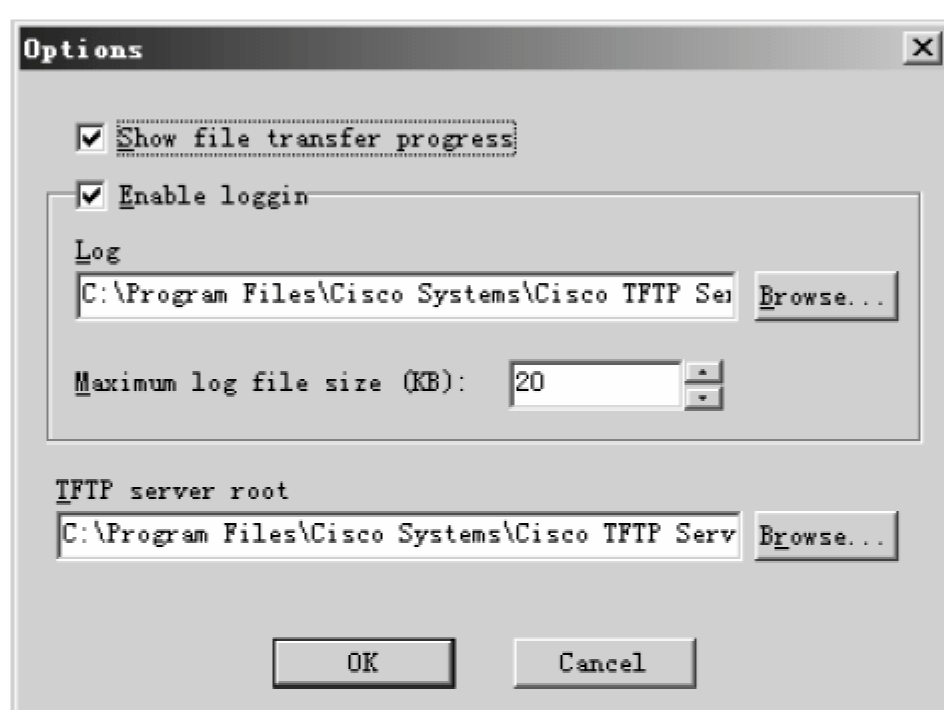


图 2-49 Cisco TFTP Server 配置

3. 连通 TFTP 服务器与路由器

在实现备份之前首先要依照图 2-44 所示的网络拓扑图连接设备，并确保设备互通，具体操作步骤如下。

01 打开 TFTP 服务器本地连接 TCP/IP 属性对话框，网卡地址配置信息如图 2-50 所示，单击【确定】按钮应用配置。

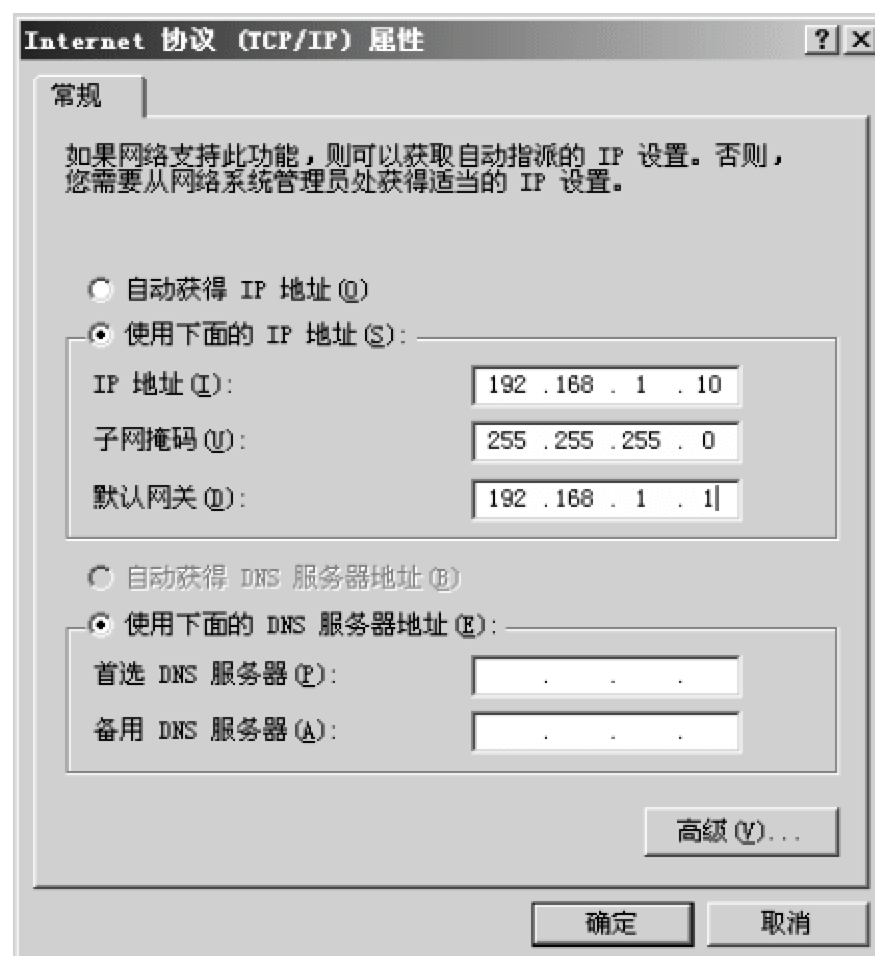


图 2-50　TCP/IP 属性对话框

02 使用 Console 口连接配置路由器，进行初始化配置，具体命令如下。

```
router(config)#int f0/0
router(config-if)#ip address 192.168.1.1 255.255.255.0
router(config-if)#no shut
```

03 在路由器上使用 ping 命令测试路由器到 TFTP 服务器的连通性，具体命令如下。

```
router#ping 192.168.1.1
type escape sequence to abort.
sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
success rate is 100 percent (5/5), round-trip min/avg/max = 36/39/44 ms
```

4. 备份配置文件到 TFTP 服务器

备份配置文件的具体操作命令如下。

```
router#copy startup-config tftp
address or name of remote host []? 192.168.1.10        //告诉 TFTP 服务器的 IP 地址
destination filename [router-confg]?              //回答文件名，默认为“路由器名-confg”
!!
1200 byte copied in 0.351 secs (3428 bytes/sec)
```

备份成功，配置文件总大小为 1200 字节，在 TFTP 程序主目录中可以找到该文件。备份的配置文件是一个纯文本文件，可以写字板打开，但使用记事本则格式会出问题。

还有一种更为简单的方法，就是采用“复制、粘贴”来进行配置文件的备份。在终端窗口内，执行“show running-cofig”命令，显示当前的配置，在终端窗口内复制全部配置，粘贴到某文本文件中。要注意的是，如果在配置中出现“--More--”等字样，一定要删除这些字符。

5. 恢复配置文件

如果路由器的配置文件不小心误删除了，可以使用备份的配置文件进行恢复，具体操作命令如下。

```
Router>en
Router#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip add 172.16.1.101 255.255.255.0
Router(config-if)#no shut
Router(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Router#copy tftp startup-config                //从 TFTP 服务器上将配置文件复制回来
Address or name of remote host []? 172.16.1.100    //TFTP 服务器 IP 地址或主机名
Source filename []? R1-confg                    //存放在 TFTP 上的配置文件名称
Destination filename [startup-config]?          //保留默认名为“startup-config”
!!!!!!!
1200 byte copied in 0.351 secs (3428 bytes/sec)
```

2.4.2 设备加密

网络设备的配置接入方法有很多种，如 Console 口配置、AUX 口拨号连接、Telnet 远程控制、HTML 网页配置。无论是哪一种方法，都有很大的权限修改设备的配置信息，如果网络设备被随意地连接则会对网络正常使用造成很大的威胁，所以这些配置接入方法一般都需要配置访问口令。下面针对网络设备的口令安全作详细的介绍。

1. 默认口令隐患多

大部分的网络设备在出厂时都有默认用户名和口令，比较常见的有 admin、guest。攻击者只要可以接入网络，就可以利用这些默认的口令登录该网络的设备进行操作。

而在现实环境中，很多网络管理员出于方便记忆和对网络安全性过于信赖等因素，一直使用默认用户名和密码，这几乎和不设密码保护没什么区别。

2. 安全口令的配置管理规范

网络设备提供了多机口令，包括常规模式口令、特权模式口令、配置模式口令、Console 控制口连接口令、Telnet 连接口令、SSH 连接口令等。在复杂的网络环境中，每一个口令都是一个安全屏障，所以在配置设备时尽量要配置所有的口令，同时各个口令的密码要有区分，以确保每一个口令都是有意义的。除此之外，不同的设备口令配置也不能相同。

在进行口令配置时，口令应具备以下特征。

（1）口令应具备复杂性，最好由数字、字母、符号 3 种字符组成。

（2）口令长度不宜过短，6~8 位以上安全性较高，不宜破解。

（3）口令不建议使用生日、人名、公司信息等具有特殊意义的字符串。

日常管理中，可以制作一套口令表，方便查看和记忆。但是，在使用时口令可能随时被卸了，所以需要管理员定期更新一些口令，并且在获悉口令泄露后及时更改口令。

3. 特权模式的口令配置

使用任何一种设备配置接入方式，都需要从用户模式进入到特权模式。如果只设置了 Telnet

远程登录密码，没有配置特权模式密码，只能进入到用户模式，所以想要通过远程连接正常配置设备，必须要配置特权模式密码。下面以 Cisco 路由器为例详细介绍一下特权模式口令的配置方法。

```
Router>enable
//进入特权模式
Router#configure terminal
//进入全局配置模式
Router(config)#enable password Cisco
//配置特权模式明文口令"Cisco"
Router(config)#enable secret Cisco
//配置特权模式密文口令"Cisco"
Router#show running-config
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password Cisco
//查看配置信息，"secret"后的"5"表示使用的是 MD5 加密认证
```

4. Telnet 远程登录口令配置

Telnet 远程登录设备时，使用的是设备的 VTY 口。网络设备默认有 5 个端口供远程终端客户机连接，也就是 0~4 5 个虚拟接口，在进行配置时要同时对 5 个虚拟接口配置登录口令。具体操作步骤如下。

```
Router(config)#line vty 0 4
//进入虚拟接口 0~4 的配置子模式
Router(config-line)#login
% Login disabled on line 66, until 'password' is set
% Login disabled on line 67, until 'password' is set
% Login disabled on line 68, until 'password' is set
% Login disabled on line 69, until 'password' is set
% Login disabled on line 70, until 'password' is set
//开启登录功能，开启后提示允许给 5 个虚拟接口配置密码
Router(config-line)#password Cisco
//配置 VTY 口令"Cisco"
Router#show running-config
line vty 0 4
 password Cisco
 login
//查看配置信息
```

5. Console 控制口安全配置

使用配置线直接连接设备配置时，使用的是串口和 Console 控制口。下面详细介绍 Console 控制口口令的配置步骤。

```
Router(config)#line console 0
//进入 Console 口的配置子模式
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
//开启登录功能，开启后提示允许给 Console 控制口配置密码
Router(config-line)#password Cisco
//配置 Console 控制口口令"Cisco"
```

```
Router#show running-config
line con 0
 password Cisco
 login
//查看配置信息
```

6. 为所有口令加密

大部分口令默认明文显示，这样很不安全，所以在配置完所有口令后，需要对设备口令进行统一加密，操作命令如下。

```
Router(config)#service password-encryption
```

加密后，使用“show running-config”命令查看配置信息。

```
Router#show running-config
service password-encryption
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password 7 0822455D0A16
!
line con 0
 password 7 0822455D0A16
 login
line vty 0 4
 password 7 0822455D0A16
 login
```

2.4.3 项目实战 3：网络设备密码恢复

当网络设备密码丢失或遗忘时，网络管理员需要想办法将密码找回或重新设置密码。对于思科设备来说，交换机和路由器密码恢复重置的操作方法大不相同，分别介绍如下。

1. 路由器密码恢复

恢复路由器密码，首先要重新启动路由器，当控制台上出现启动过程时，迅速按 Ctrl+Break 组合键，中断路由器的启动过程，进入 rommon 模式。

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by Cisco Systems, Inc.
Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :
#######
monitor: command "boot" aborted due to user interrupt
rommon 1 >confreg 0x2142       //改变配置寄存器的值为 0x2142，使路由器在启动时不加载 NVRAM 中的
                               //startup-config 配置文件
rommon 2 >boot                 //重新启动路由器
Router>enable                  //重新启动后不需要密码
Router#copy startup-config running-config     //把配置文件从 NVRAM 中复制到 RAM 中
Destination filename [running-config]?
```

```
432bytes copied in 0.403 secs (1122 bytes/sec)
Router#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#enable password Cisco          //修改新的特权模式明文密码（其他密码用类似方法重设）
Router(config)#config-register 0x2102         //把寄存器的值修改为正常值
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#write            //保存配置修改
Destination filename [startup-config]?
Building configuration...
[OK]
Router#reload              //重新启动路由器
```

2. Cisco 交换机密码恢复

恢复交换机密码时同样需要重新启动设备，接通交换机电源后马上按下面板上的 mode 键，持续 6 秒以上，直到进入交换机 boot 模式为止。进入迷你系统后的操作命令如下。

```
>flash_init                                   //此时已经进入交换机 boot 模式，初始化 flash
>rename flash:config.text flash:config.old    //将还有 password 的配置文件名修改，使设备启动时不加载该配
                                              //置文件
>reboot                                         //重新启动交换机
Switch>enable                                   //重新启动不需要密码登录
Switch #rename flash:config.old flash:config.text    //把配置文件名改回来
Switch #copy startup-config running-config          //把配置文件从 NVRAM 中复制到 RAM 中
```

下面参照恢复路由器密码的方式，重新配置交换机各种密码即可。

2.4.4　项目实战 4：设备 IOS 的备份、恢复和更新

设备的 IOS（镜像）如计算机的操作系统一样，是设备得以使用的软件组成，在日常使用中很有可能会出现 IOS 损坏的现象，所以需要在设备购买后先将其 IOS 进行备份。同时产品出厂后很有可能存在漏洞，所以很多厂商都会对设备 IOS 进行定期的更新，作为管理员也应当及时关注设备更新。

下面分别介绍设备 IOS 备份与恢复的具体操作方法。

1. 实验拓扑

本实例采用如图 2-9 所示网络拓扑图连接设备，依图所示进行连通性配置。

2. 备份 IOS 到 TFTP 服务器

IOS 主要存在于设备的 Flash 闪存中，所以只要将 Flash 中的 IOS 文件备份到 TFTP 服务器即可，具体操作步骤如下。

01　查看 IOS 镜像文件，操作命令如下。

```
router#show flash
system flash directory:
file   Length     Name/status
```

```
   1     5571584    c2600-i-mz.122-28.bin
[5571584 bytes used, 58444800 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
//查看 Flash 中的 IOS 大小和文件名等
```

02 使用 copy 命令备份 IOS 文件到 TFTP 服务器，操作命令如下。

```
router#copy flash:c2600-i-mz.122-28.bin tftp          //把 IOS 备份到 TFTP 服务器上
address or name of remote host []? 192.168.1.10        //TFTP 服务器 IP 地址
destination filename [c2600-i-mz.122-28.bin]?        //回答文件名。默认和源文件名一致，不建议改变文件名，
                                                     //因为 IOS 文件名包含了 IOS 的版本和特征等信息
……（此处省略）
//备份成功后，可以在文件根目录里寻找到
```

3. 恢复 IOS

为了演示实验，这里故意删除 Flash 中的 IOS 文件，以便进行 IOS 的恢复操作。

01 查看 IOS 镜像文件，操作命令如下。

```
router#show flash
system flash directory:
file    Length      Name/status
   1     5571584    c2600-i-mz.122-28.bin
[5571584 bytes used, 58444800 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
//查看 Flash 中的 IOS 大小和文件名等
```

02 使用 delete 命令删除 Flash 中的 IOS 文件，操作命令如下。

```
R1#delete flash:c2600-i-mz.122-28.bin
Delete filename [c2600-i-mz.122-28.bin]?
Delete flash:/c2600-i-mz.122-28.bin? [confirm]
```


提 示

进行以上操作时要慎重。如果工作中不慎误删了 IOS，不要关闭路由器，立刻使用 copy tftp flash 命令从 TFTP 服务器把 IOS 恢复过来。为了从 TFTP 服务器恢复 IOS，还可以用 Xmodem 方式通过 Console 口进行恢复，然而 Console 的速度很慢，很少被采用。

03 如果 IOS 丢失后，路由器重新启动将进入 rommon 模式，在 rommon 模式下将 IOS 从 TFTP 服务器恢复的操作命令如下。

```
SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by Cisco Systems, Inc.
Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Boot process failed...
The system is unable to boot automatically.   The BOOT
environment variable needs to be set to a bootable
image.
rommon 1 > IP_ADDRESS=192.168.1.1                //路由器 IP 地址
```

```
rommon 2 > IP_SUBNET_MASK=255.255.255.0        //子网掩码
rommon 3 > DEFAULT_GATEWAY=192.168.1.10        //路由器网关地址
rommon 4 > TFTP_SERVER=192.168.1.10            //TFTP 服务器 IP 地址
rommon 5 > TFTP_FILE= c2600-i-mz.122-28.bin    //TFTP 可用于恢复的 IOS 文件
```


提 示

要恢复 IOS，需要配置一些变量的值，主要是路由器的 IP 地址、掩码等。由于这里的路由器和 TFTP 服务器在同一网段，是不需要网关的，但是不能不配置该值，所以就指向了 TFTP 服务器。注意变量的大小写。

```
rommon 8 > tftpdnld      //开始恢复 IOS
          IP_ADDRESS: 192.168.1.1
      IP  SUBNET  MASK: 255.255.255.0
     DEFAULT  GATEWAY: 192.168.1.10
         TFTP  SERVER: 192.168.1.10
           TFTP_FILE: SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)Copyright (c) 2000 by Cisco Systems, Inc.Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes o
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:   [n]:   y
//回答“y”开始从 TFTP 服务器上恢复 IOS
Receiving                    c2600-i-mz.122-28.bin            from
192.168.1.10!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Validating checksum.
Copying file c2600-i-mz.122-28.bin to flash.
Eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
//从 TFTP 服务器接收到 IOS 后，会进行校验
rommon 9 > boot                         //重新启动 IOS
```

2.4.5　项目实战 5：Telnet 远程管理多个设备

在进行网络设备管理、配置或故障调试时，经常会遇到在多台设备之间来回切换配置的现象，除了初始配置外，后期的大多数配置都是使用 Telnet 远程管理，而一般的 Telnet 连接在切换设备时都需要先退出当前连接才可以连接下一台设备，这样的话每切换一次设备都有可能要重新进行 Telnet 连接，很浪费时间。所以 Cisco 提出了一种同时连接多台设备随意切换的方式。具体操作方法如下。

1. 网络拓扑图

本实验可依照图 2-52 所示的网络拓扑图进行设备连接。

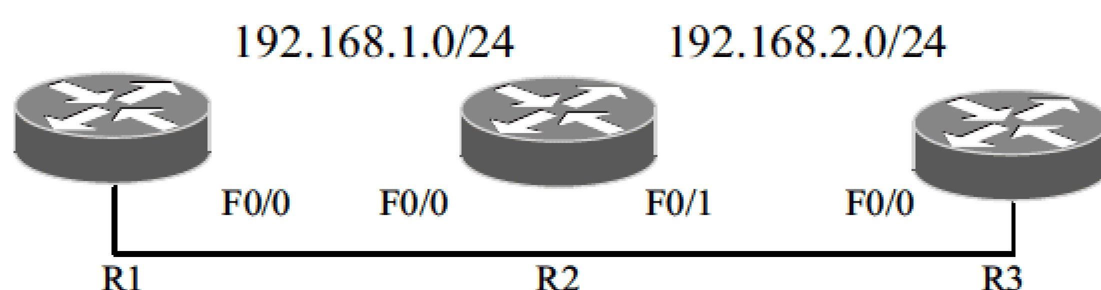


图 2-52　Telnet 远程管理多台设备实验拓扑

2. 设备环境配置

为了达到实验目的，需要为设备进行相应的配置，具体命令配置如下。

01 初始化 3 台路由器的配置，进行设备命名及端口配置。

R1：

```
router>enable
router#configure terminal
router(config)#hostname R1
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config)#interface loopback 0
//配置虚拟接口“loopback 0”，此接口地址作为设备管理地址使用
R1(config-if)#ip add 1.1.1.1 255.255.255.0
```

R2：

```
router(config)#hostname R2
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shut
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config)#interface loopback 0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
```

R3：

```
router(config)#hostname R3
R3(config)#interface f0/0
R3(config-if)#ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shut
R3(config)#interface loopback 0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
```

02 为配置 RIP 路由协议，确保网络互通。

R1:

```
R1(config)#router rip
//配置 RIP 路由协议
R1(config-router)#version 2
//路由协议使用 RIPv2 版本
R1(config-router)#network 192.168.1.0
//通告网段“192.168.1.0”
R1(config-router)#network 1.1.1.0
//通告网段“1.1.1.0”
R1(config-router)#no auto-summary
//取消子网汇总
```

R2:

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 2.2.2.0
R2(config-router)#no auto-summary
```

R3:

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.2.0
R3(config-router)#network 3.3.3.0
R3(config-router)#no auto-summary
```

03 开启 3 台设备 Telnet 服务。

```
R1(config)#line vty 0 4
R1(config-line)#login
% Login disabled on line 66, until 'password' is set
% Login disabled on line 67, until 'password' is set
% Login disabled on line 68, until 'password' is set
% Login disabled on line 69, until 'password' is set
% Login disabled on line 70, until 'password' is set
R1(config-line)#password Cisco
```

3 台设备的配置命令完全一样，所以只使用 R1 进行演示。

04 配置特权模式访问密码。

Telnet 登录设备后必须要有特权模式的密码才能配置设备，一般会采用明文或密文两种密码，操作命令如下。

```
R1(config)#enable password Cisco
//配置特权模式明文密码为“Cisco”
R1(config)#enable secret Cisco
//配置特权模式密文密码为“Cisco”
```

3. 测试管理多台设备

```
R1#telnet 2.2.2.2           //在 R1 上 Telnet R2，“2.2.2.2”为 R2 的设备管理地址
Trying 2.2.2.2 ...Open

User Access Verification

Password:                   //输入登录 R2 的 Telnet 密码，密码为“Cisco”，输入不显示
R2>enable
Password:                   //输入登录 R2 特权模式密码，密码为“Cisco”，输入不显示
R2#                         //进入 R2 特权模式
R1#                         //在 R2 的特权模式同时按下 Ctrl+Shift+6 组合键，松开后马上按 X 键，可将 TelnetR2
                            //的连接挂起，并返回 R1 的特权模式

R1#telnet 3.3.3.3           //在 R1 上 Telnet R3，“3.3.3.3”为 R3 的设备管理地址
Trying 3.3.3.3 ...Open
```

```
User Access Verification

Password:
R3>enable
Password:
R3#                 //进入 R2 特权模式，同时按下 Ctrl+Shift+6 组合键，松开后马上按 X 键，将 Telnet R2 的
                    //连接挂起，并返回 R1 的特权模式
R1#sh sessions      //查看已挂起的 Telnet 连接
Conn Host             Address          Byte   Idle Conn Name
   1 2.2.2.2          2.2.2.2          0      0 2.2.2.2
*  2 3.3.3.3          3.3.3.3          0      0 3.3.3.3
                    //“Conn”表示连接编号，可以看到有两个已挂起连接
R1#1                //在特权模式下直接输入需要登录的设备连接编号，连续两次按 Enter 键，
                    //可快速切换到指定设备
```

2.4.6 项目实战 6：使用脚本快速配置多台网络设备

在现实网络环境中，网络设备的配置内容比较多，整个网络由网络工程师全部配置下来工作量会很大，而且其中大多数网络设备的基本配置都相似。为了减少工作量，网络管理员可以考虑将相似的设备配置定义为脚本程序，让设备快速获得基本配置。具体操作方法如下。

1. 实验拓扑

本实例采用如图 2-53 所示的网络拓扑图连接设备，依图所示进行连通性配置。

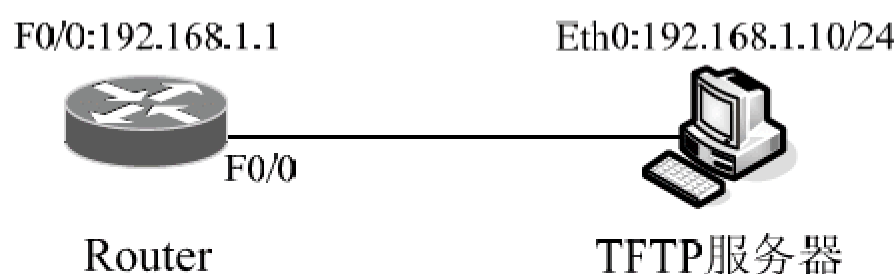


图 2-53　实验拓扑图

2. 实验步骤

快速配置多台网络设备的方法如下。

01 按照图 2-53 所示的网络拓扑图，连接网络设备，在客户机上安装 TFTP 程序。

02 完成 Router 路由器的所有配置内容，确保路由器和 TFTP 服务器互通。使用 copy startup-config tftp 命令，将 Router 的配置保存到 TFTP 服务器。

```
Router#copy startup-config tftp                    //保存已经配置好的路由器的配置文件
Address or name of remote host []? 192.168.1.10    //指定 TFTP 服务器 IP 地址
Destination filename [Router-confg]?               //指定配置文件保存后的文件名，默认名为 Router-confg

Writing startup-config....!!                       //开始保存数据
[OK - 465 bytes]

465 bytes copied in 3.089 secs (0 bytes/sec)
Router#
```

03 按照其他设备的配置需求修改已保存的配置文件。

04 使用 copy tftp startup-config 命令将修改过的配置文件导入指定设备。

```
Router#copy tftp startup-config                    //复制修改过的配置文件到路由器
Address or name of remote host []? 192.168.1.10    //指定 TFTP 服务器 IP 地址
Source filename []? Router-confg                   //指定修改的配置文件名
Destination filename [startup-config]?             //指定保存到路由器后的目标文件名，采用默认配置"startup-config"

Accessing tftp://192.168.1.10/Router-confg...
Loading Router-confg from 192.168.1.10: !
[OK - 465 bytes]

465 bytes copied in 0.032 secs (14531 bytes/sec)
Router#
```

05 使用 show 命令检查设备配置，并对不合适的配置内容进行调整。

06 依照以上步骤完成其他配置相似的设备配置。

2.4.7 设备连通测试命令——ping

ping 命令经常用来测试网络设备的连通性，是使用得比较普遍的一个命令。当两台设备能够 ping 通时才有可能传输数据，下面介绍 ping 的使用方法。

1. 普通的 ping 命令用法

简单的 ping 命令基本可以满足大部分的测试需求，它已经规定好了 ping 的源地址、数据包数量、大小等值，具体操作命令如下。

```
Router#ping 192.168.1.100                          //ping 目标设备 IP 地址
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100 timeout is 2 seconds:
!!!!!                                //感叹号表示 Ping 通
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/115/212 ms
```

2. 扩展 ping 命令用法

在某些环境下简单的 ping 并不适用，对于需要制定源地址、数据包数量和大小等参数的 ping 测试，可以使用扩展 ping，具体操作命令如下。

```
Router#ping
Protocol [ip]:                                     //所使用的协议
Target IP address: 3.3.3.3                         //目标 IP 地址
Repeat count [5]:                                  //ping 次数
Datagram size [100]:                               //数据包大小
Timeout in seconds [2]:                            //超时时间
Extended commands [n]: y
Source address or interface: 23.0.0.1              //源地址
Type of service [0]:                               //服务类型
Set DF bit in IP header? [no]:                     //是否分片
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:   //疏松、严格的路由选择，时间戳
```

```
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 23.0.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/85/216 ms
```

2.5 专家答疑

（1）本章使用的常用设备配置管理方法是否适合其他类型的产品呢？

答：网络设备厂商比较多，每个厂商都有自己的一套配置命令，但是无论哪个厂商的设备所使用的网络技术都是相似的。在掌握了基本的网络设备管理配置方法后，其他设备的配置管理方法和命令很多只是命令的词语更换，或者操作配置方法有些细微差异。

（2）设备有出厂自带的 IOS 镜像，在使用中有必要更换 IOS 镜像吗？更换时需要注意哪些事项？

答：每一个产品生产之后都会有漏洞，而且后期也有可能针对此产品进行性能的提升，所以有很多产品在上市之后都会定期地发布更新升级的 IOS 镜像，作为管理员应当做好及时的更新工作，以防止因漏洞造成的设备攻击，或者使用新 IOS 镜像让设备发挥更好的性能。

在更换 IOS 时首先要保存原有的 IOS 镜像文件，以防止更新的 IOS 镜像不兼容，备用恢复。同时存放 IOS 镜像的主要设备的 Flash 闪存，更新时一定要检测 Flash 空间，避免空间不足造成的更新失败。

第 3 章　常用网络工程配置实例

在网络工程搭建，或日常的网络管理中，网络设备总有那么几个典型的配置内容，如 VLAN 配置、ACL 访问控制列表配置、QoS 服务质量配置等，对于管理员来说这些典型的配置案例必须非常熟悉，本章将逐一介绍这些典型的网络设备配置案例。

3.1　优化局域网环境

大部分企业内部网络都是由交换机组成的局域网环境，随着企业内部网络的不断扩大，局域网扩充带来了很多问题，比较明显的有广播风暴、地址冲突。除此之外，局域网内部通信限制少，为病毒、木马等网络威胁提供了较宽松的传播环境，影响了网络安全。因此局域网环境优化在网络管理中先的尤为重要。

网络管理员需要掌握的局域网优化技术有 VLAN 技术、MAC 地址绑定技术、访问控制等，这里着重介绍前两种。

3.1.1　使用 VLAN 技术

VLAN（Virtual Local Area Network）的中文名为“虚拟局域网”，是相对物理局域网而言的，使用该技术可以将现有的由交换机互连的局域网划分成几个逻辑的虚拟局域网，虚拟局域网之间相互隔离，属于不同的广播域。这样一来可以将大的局域网构成的广播域划分成多个小的广播域，相对的广播流量会减少，缓解了广播风暴。同时 VLAN 技术还对各个虚拟局域网起到了安全隔离的效果。

1. VLAN 技术的配置

配置 VLAN 的方法有很多，可以通过指定交换机接口、客户机 MAC 地址或 IP 地址等多种方法划分 VLAN，其中用得最多的是划分交换机物理接口。如图 3-1 所示，将交换机 F0/2 接口分配给 VLAN2。

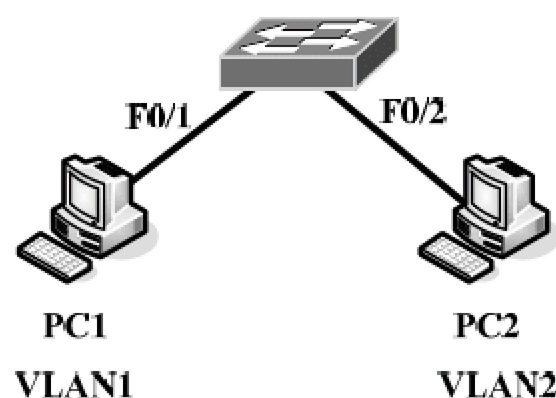


图 3-1　划分接口到 VLAN

VLAN 的操作内容主要有创建、命名、接口指派等，具体命令配置如下。

（1）创建 VLAN。

```
Switch-A#VLAN database       //进入 VLAN 配置数据库
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch-A(VLAN)#VLAN 2         //创建 VLAN2
VLAN 2 added:
    Name: VLAN0002       //默认 VLAN2 名称
```

（2）为 VLAN 命名。

```
Switch-A(VLAN)#VLAN 2 name office       //为 VLAN2 命名为“office”
VLAN 2 modified:
    Name: office
```

（3）接口指派。

```
Switch (config)#interface f0/2
Switch(config-if)#switchport access VLAN 2     //将 F0/2 接口分配给 VLAN2
```

2. VLAN 中继

在没有配置 VLAN 之前，由交换机互连的网络默认同属于 VLAN1。VLAN1 也是默认的本征 VLAN。本征 VLAN 是指交换机允许默认传输信息的 VLAN。如图 3-2 所示，两台交换机互连，所有客户端默认都属于 VLAN1。

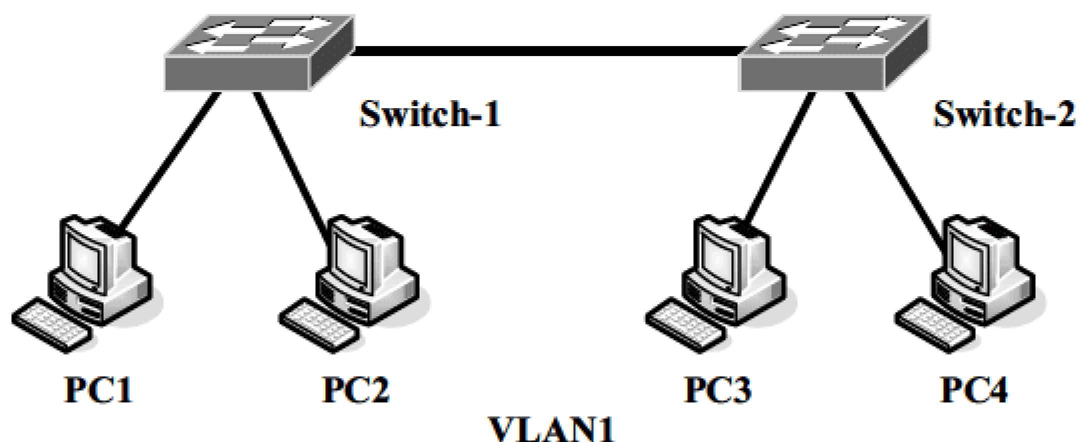


图 3-2　默认 VLAN 配置

对于不是本征 VLAN 的其他 VLAN 默认是不允许在交换机之间传输信息的。如图 3-3 所示，拓扑配置 VLAN，PC2 和 PC4 同属于 VLAN2，需要通过交换机之间的链路进行通信，但是默认链路不允许除本征 VLAN 以外的其他 VLAN 通过，那么横跨两个交换机同属于 VLAN2 的客户机就无法互通信息。

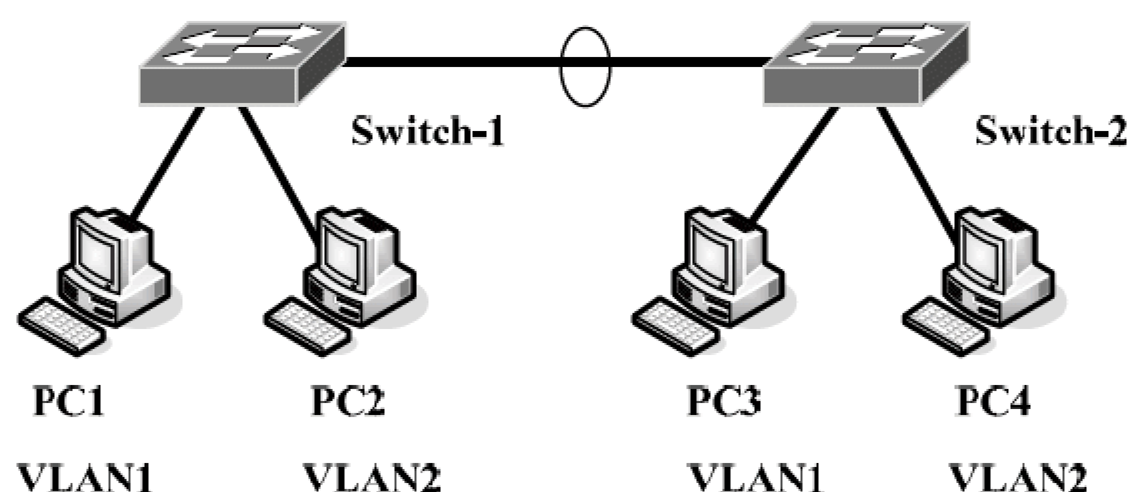


图 3-3 VLAN 中继链路

为了解决链路通过多条 VLAN 的问题，交换机的端口被定义为几种模式，分别是 access（访问模式）、trunk（中继模式）、dynamic（自协商模式）。

（1）access（访问模式）：连接客户端的接口一般为 access 模式。

（2）trunk（中继模式）：当链路需要通过多个 VLAN 时，该链路必须为 trunk 链路。

（3）dynamic（自协商模式）：自动协商，当一端为 trunk 时，另一端自动为 trunk。

将端口配置为 trunk 模式的操作命令如下。

```
Switch-1(config)#interface f0/0
Switch-1(config-if)#switchport mode trunk      //开启 trunk 模式
```



提 示

如果端口默认为自协商 auto 模式，不能直接配置 trunk，会弹出如下提示信息。“Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.”可以先使用“switchport mode access”命令将端口配置成 access 模式，再使用“switchport mode trunk”命令开启 trunk 模式。

```
Switch-1(config-if)#switchport trunk native VLAN [VLAN ID]    //配置本征 VLAN，默认为 VLAN1
Switch-1(config-if)#switchport trunk allowed VLAN [WORD/add/all/except/none/remove]
//指定 trunk 链路允许通过的 VLAN，默认允许通过所有 VLAN，【WORD】指定 VLAN 名，【add】添加 VLAN，
//【all】允许所有 VLAN，【except】除此之外的所有 VLAN，【none】禁止所有 VLAN 通过，【remove】移除某一 VLAN
```

3. VTP

在大型的局域网中，涉及的 VLAN 数量可能会很多，日常的管理维护工作相对也比较繁重，单靠人工操作难免会影响工作效率。为此 Cisco 提出了 VTP（VLAN 中继协议），利用该协议可以实现快速的地址配置。

VTP 的工作原理是，将少数设备定义为服务器，其他设备定义为客户端，在服务器上配置所有 VLAN，并自动向所有信息匹配的客户端分发 VLAN 配置信息。对 VLAN 进行配置调整时只需要在服务器设备进行操作即可。

VTP 配置时可以将设备定义为 3 种工作模式，分别是服务器模式、客户端模式、透明模式。

（1）服务器模式：可以添加、删除、修改 VLAN 信息，并且可以向其他服务器模式的设备学习 VLAN 配置信息。

（2）客户端模式：只能向服务器模式的设备学习 VLAN 配置信息。

（3）透明模式：可以添加、删除、修改 VLAN 信息，但是不学习服务器设备的 VLAN 配置

信息。可以转发服务器设备的 VLAN 配置信息。

3.1.2 使用 MAC 地址绑定技术

在网络环境中经常会出现地址冲突、地址欺骗的现象。某些终端客户机因手工配置或感染木马等，使自己的地址信息和服务器或其他主机地址信息发生冲突，进而影响到整个网络的正常使用，如常见的 ARP 地址欺骗。

普通主机之间发生冲突，可能影响不是很大，主机提示冲突后重新配置新地址就可以了。但是有些服务器或网络设备在网络中的位置至关重要，一旦出现地址冲突，会对网络业务服务造成巨大的影响，如 Web 服务器、设备管理地址、网关等。

下面主要介绍几种常用的地址绑定方法。

1. 基于端口的 MAC 地址绑定

可以通过规定某一接口允许通过的 MAC 地址来实现绑定。下面以 Cisco 2950 交换机为例进行配置。

```
Switch>enable
//进入特权模式
Switch#configure terminal
//进入全局配置模式
Switch(config)#interface fastEthernet 0/1
//进入 fastEthernet 0/1 端口的配置子模式
Switch(config-if)#switchport port-security
//配置开启端口安全模式
Switch(config-if)#switchport port-security mac-address 0001.AB3D.32EA
//将某主机的 MAC 地址“0001.AB3D.32EA”绑定到该端口，允许主机通过该端口访问网络
Switch(config-if)#no switchport port-security mac-address 0001.AB3D.32EA
//删除绑定主机的 MAC 地址“0001.AB3D.32EA”
Switch(config-if)#switchport port-security maximum 30
//最大允许验证通过的 MAC 地址数，本实例设为“30”
```


提 示

如果在开启端口安全模式时，弹出“Command rejected: FastEthernet0/1 is a dynamic port”提示，说明当前接口模式为 dynamic，不能开启端口安全。需要在接口子配置“switchport mode access”命令，将接口改为 access 模式。

2. 基于扩展访问控制列表的 MAC 地址绑定

平时接触的访问控制列表大都是基于 IP 地址和端口的，而基于 MAC 地址也可以实现访问控制功能，进而实现 MAC 地址绑定。下面以 Cisco 3560 交换机为例进行配置。

（1）创建访问控制列表。

```
Switch(config)#Mac access-list extended MAC
//创建一个 MAC 地址访问控制列表，并命名为 MAC
Switch(config-ext-macl)#permit host 0001.AB3D.32EA any
//定义 MAC 地址为“0001.AB3D.32EA”的主机可以访问任意主机
```

```
Switch(config-ext-macl)#permit any host 0001.AB3D.32EA
//定义所有主机可以访问 MAC 地址为"0001.AB3D.32EA"的主机
```


提 示

默认在访问控制列表最后有一条“deny any any”隐藏命令，以拒绝其他所有 MAC 地址的访问请求。

（2）应用访问控制列表。

```
Switch(config)#interface fastEthernet 0/1
//进入 fastEthernet 0/1 端口配置子模式
Switch(config-if)#mac access-group MAC in
//在 fastEthernet 0/1 端口应用访问控制列表"MAC"
```

（3）删除访问控制列表。

```
Switch(config)#no mac access-list extended MAC
```

3. 基于 IP 地址和 MAC 地址的绑定

在很多网络环境下，IP 地址是不可以随意更改使用的，变更 IP 地址很容易造成地址盗用或冲突。例如，某一 IP 地址在网络中具有访问其他资源的特权，一旦被不法分子在其他主机盗用就麻烦了。

如果只使用前两种方式，只能限制允许通过的 MAC 地址，但是达不到 MAC 和 IP 地址绑定的功能。必须想办法让 IP 地址和 MAC 地址一一对应起来。下面介绍详细配置方法。

使用 ARP 命令绑定 IP 和 MAC 对应关系，将 IP 地址“192.168.100.100”和 MAC 地址“0001.AB3D.32EA”绑定在一起。

```
Router(config)#arp 192.168.100.100 0001.AB3D.32EA ARPA
```

4. 基于 IP 地址和交换机端口的绑定

可以将 IP 地址与交换机端口也绑定在一起，这样一来该端口就只能由对应的 IP 地址使用，使用其他 IP 地址连接会立刻断网，有效地防止了乱改 IP 的行为。下面介绍详细的配置方法。

```
Router(config)#access-list 1 permit 192.168.100.100
//定义一条允许 IP 地址"192.168.100.100"通过的访问控制列表，编号为 1
Router(config)#interface fastethernet0/1
//进入需要实施绑定的端口"fastethernet0/1"的配置子模式
Router(config-if)#ip access-group 1 in
//在端口配置子模式下应用访问控制列表 1
配置后在 fastethernet0/1 端口只允许 IP 地址 192.168.100.100 的主机连接网络
```

3.1.3 项目实战 1：使用 VTP 快速配置 VLAN

VLAN 配置在大型局域网络中使用很普遍，下面演示一个使用 VTP 快速配置 VLAN 的实例。

1. 网络拓扑图

本实验可依照图 3-4 所示的网络拓扑图进行设备连接。

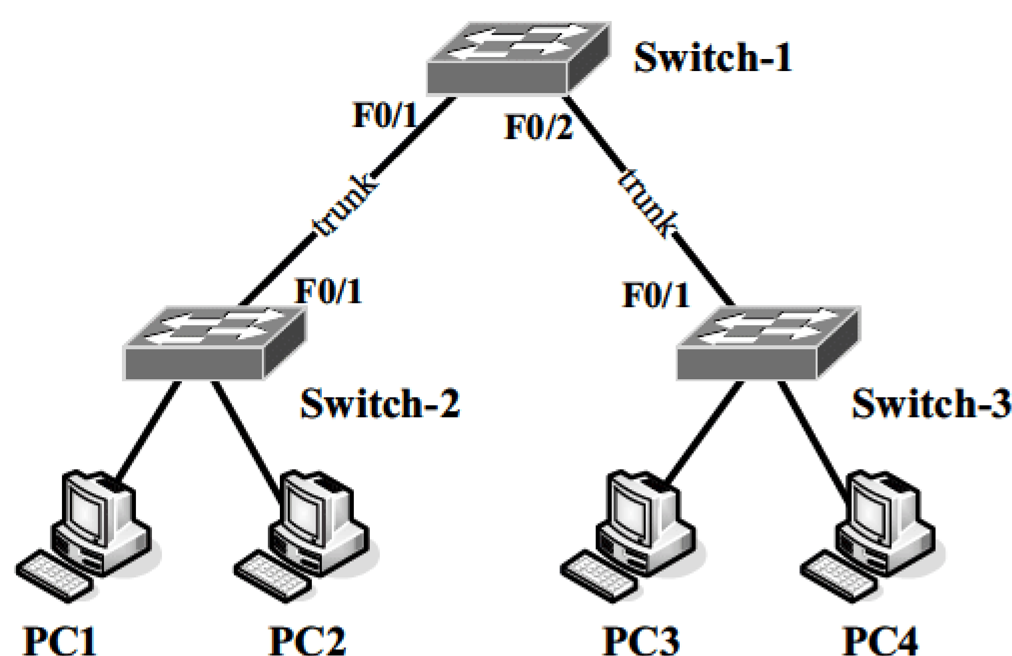


图 3-4　VTP 配置的网络拓扑图

2. 项目配置

使用 VTP 协议配置 VLAN 的具体操作步骤如下。

01 在 Switch-1 上创建 VLAN2~5，具体操作命令如下。

```
Switch-1#VLAN database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch-1(VLAN)#VLAN 2
VLAN 2 added:
    Name: VLAN0002
Switch-1(VLAN)#VLAN 3
VLAN 3 added:
    Name: VLAN0003
……
Switch-1(VLAN)#VLAN 5
VLAN 10 added:
    Name: VLAN0010
```

02 在三台交换机上分别配置 VTP 协议，将 Switch-1 配置为 VTP 服务器模式，Switch-2 和 Switch-3 作为客户端，具体操作命令如下。

Switch-1：

```
Switch-1(VLAN)#vtp server       //定义 Switch-1 为 VTP 服务器模式
Device mode already VTP SERVER.
Switch-1(VLAN)#vtp domain Cisco     //定义 VTP 域，服务器和客户端需要在同一个域中
Changing VTP domain name from NULL to Cisco
Switch-1(VLAN)#vtp password Cisco     //定义 VTP 验证密码，服务器和客户端密码要一致
Setting device VLAN database password to Cisco
```

Switch-2：

```
Switch-2(VLAN)#vtp domain Cisco
Domain name already set to Cisco.
Switch-2(VLAN)#vtp server
Device mode already VTP SERVER.
```

```
Switch-2(VLAN)#vtp password Cisco
Setting device VLAN database password to Cisco
```

Switch-3：

```
Switch-3(VLAN)#vtp domain Cisco
Domain name already set to Cisco.
Switch-3(VLAN)#vtp server
Device mode already VTP SERVER.
Switch-3(VLAN)#vtp password Cisco
Setting device VLAN database password to Cisco
```

03 因为 VTP 信息只在 trunk 接口上发送，所以先将交换机相连的接口配置成 trunk 接口，操作命令如下。

Switch-1：

```
Switch-1(config)#int f0/1    //如果交换机支持多种 VTP 封装的话，则需要先指定封装
Switch-1(config-if)#switchport trunk encapsulation dot1q      //2950 上无此命令
Switch-1(config-if)#switchport mode trunk
Switch-1(config)#int f0/2
Switch-1(config-if)#switchport trunk encapsulation dot1q
Switch-1(config-if)#switchport mode trunk
```

Switch-2：

```
Switch-2(config)#int f0/1
Switch-2(config-if)#switchport trunk encapsulation dot1q
Switch-2(config-if)#switchport mode trunk
```

Switch-3：

```
Switch-3(config)#int f0/1
Switch-3(config-if)#switchport trunk encapsulation dot1q
Switch-3(config-if)#switchport mode trunk
```

04 验证 VTP，在 Switch-2 上查看 VLAN 信息，看是否可以看到 Switch-1 创建的 VLAN 信息。

```
Switch-2#show VLAN

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
2    VLAN0002                         active
3    VLAN0003                         active
4    VLAN0004                         active
5    VLAN0005                         active
1002 fddi-default                     act/unsup
```

```
1003 token-ring-default              act/unsup
1004 fddinet-default                 act/unsup
1005 trnet-default                   act/unsup
```



提 示

VTP 在进行分配 VLAN 信息时，默认客户端会学习到所有的 VLAN 信息，但是客户端并不一定需要使用所有的 VLAN。对于客户端没有使用的 VLAN，可以使用 VTP 修剪功能将其清除，以减小客户端的负担。VTP 修剪的命令为“vtp pruning”。

3.2 使用冗余技术提高网络可用性

网络的可用性是至关重要的，经常会出现因网络设备、链路损坏而导致整个网络瘫痪的现象。为了解决这个问题，需要在原来已有的链路基础上再增加一条备用链路，当一条链路因故障损坏后，另一条链路依然可以工作，这称作网络冗余。

但是直接增加链路可能会导致网络环路，造成广播风暴，所以要配合相应的技术来实现网络冗余。一般常用的网络冗余技术可以分作二层链路冗余和三层网关冗余，具体内容介绍如下。

3.2.1 运用 STP 提供二层链路冗余

STP- Spanning Tree Protocol（生成树协议），是局域网环境中普遍使用的网络冗余技术。STP 协议的工作原理是，逻辑上断开环路中的一条链路，防止广播风暴产生，当线路故障时自动激活被逻辑断开的链路，恢复通信。其中逻辑断开的链路称作备份链路。

如图 3-5 所示，为了确保网络有冗余链路，三台交换机互连构成一个环路，并使用 STP 协议以避免广播风暴，其中 Switch-B 和 Switch-C 之间的链路“c”为逻辑断开的链路，当“a”和“b”任意一条链路出现故障时，链路“c”会自动激活，以确保 Switch-B 和 Switch-C 正常通信。

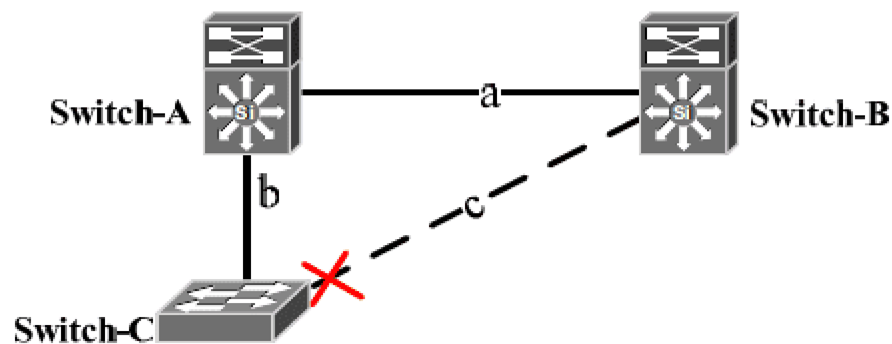


图 3-5　STP 网络拓扑图

为什么图 3-5 示环路中的链路“c”为逻辑断开的链路呢？是否断开任意一条链路都可以呢？

在 STP 生成树中，断开的链路并不是随意选择的，而是通过设备、接口、链路优先级决定哪条链路逻辑断开的。具体选择原则如下。

首先在局域网中找一台设备作为根桥，根桥由桥 ID 的大小决定，桥 ID 值最小的设备为根桥。桥 ID=桥优先级+桥 MAC 地址，其中“桥”就是“网桥”，即交换机。默认情况下交换机的的优先级都是 32768，如果需要某一台设备为根桥的话，直接将其优先级改小即可，不过交换机的优先级规定必须为 4096 的倍数。

如图 3-6 所示，交换机 SW2 的优先级为 4096，所以该交换机为根桥。根桥确定后，交换机 SW3

到达根桥有两条路径，要根据两条链路的成本值决定应该逻辑断开哪一条。网桥到根网桥的成本等于路径上所有链路的成本之和，可参照表 3-1 计算成本。

表 3-1　链路成本对照表

链路带宽（Mbps）	路径成本	链路带宽（Mbps）	路径成本
10	100	155	14
16	62	622	6
45	39	1000	4
100	19	10000	2

由图中可以看出所有链路都是 100M 链路，所以 SW2 和 SW3 直连链路总成本较低，应该保持。而考虑交换机 SW1 到达根的链路问题，图中 SW1 和 SW3 直连链路应该作为逻辑断开链路，备份使用。

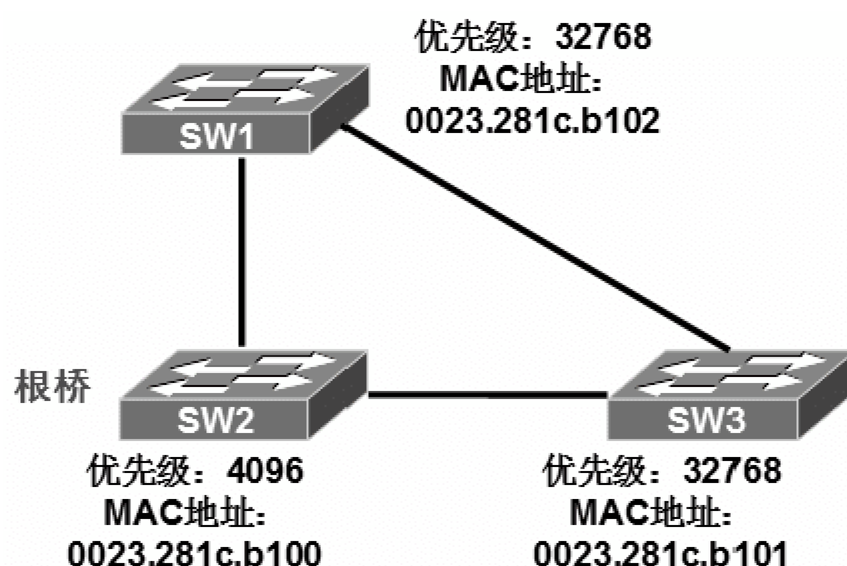


图 3-6　STP 案例拓扑图

3.2.2　使用 VRRP 提供三层网关冗余

VRRP（虚拟路由冗余协议）和 HSRP（热备份路由协议）都是比较常用的网关冗余方法。两种方法的原理都是在一组真实路由器中构建虚拟路由器，只要有一条物理链路畅通，虚拟路由器就可以作为网关被客户端使用，确保了网络的可用性。但是 HSRP 协议是思科专属的，VRRP 协议是开放的，所以在设备比较复杂的网络里，大都使用 VRRP 协议实现网关冗余。

使用 VRRP 协议产生的虚拟路由器会被配置一个 IP 地址，该地址被指定为内网网关。虚拟路由器可动态地分配到配置 VRRP 协议的物理路由器上，获得 VRRP 虚拟路由器身份的物理路由器称为 VRRP 的主路由器，它将负责转发内网客户端的请求数据包。一旦主路由器故障，VRRP 协议会动态地将虚拟路由器身份分配给另一台配置 VRRP 的物理路由器，使其成为主路由器。

VRRP 进行主路由器身份选择时，主要通过 VRRP 优先级决定，优先级范围为 1~255，默认优先级为 100，选择优先级高的设备为主路由器。如果设置为 0 则代表该设备不参与 VRRP 选择，可通过为主路由器配置 0 优先级而让其自动“辞职”。

VRRP 协议定义了三种状态模型，分别是初始状态（Initialize）、活动状态（Master）和备份状态（Backup）。开始运行 VRRP 时，处于初始状态，获得虚拟路由器身份的主路由器处于活动状态，当主路由器故障时可抢夺主路由器身份的路由器处于备份状态。

在配置 VRRP 时，不一定非要使用路由器，具有路由功能的三层交换机也可以实现。在使用三层交换机时，如果有两个三层交换机，配置了 VLAN1~10 的虚拟局域网，可以针对局域网中的

不同 VLAN 配置 VRRP，调整优先级，使 VLAN1~5 中的主路由器身份和 VLAN6~10 中的主路由器身份有所差异，这样可以实现整个网络流量的负载均衡。

3.2.3 项目实战 2：使用三层交换机实现基于 VLAN 的多层冗余

网络冗余是当前网络为了提高可用性、稳定性必不可少的技术。特别是局域网环境比较大的企业网络中，通常会使用双核心交换机互做备份，实现二层交换网络冗余和三层出口网关冗余。下面模拟一套基于 VLAN 的多层网络冗余实例，具体内容介绍如下。

1. 实验拓扑图

可依照图 3-7 所示网络拓扑图进行实验。

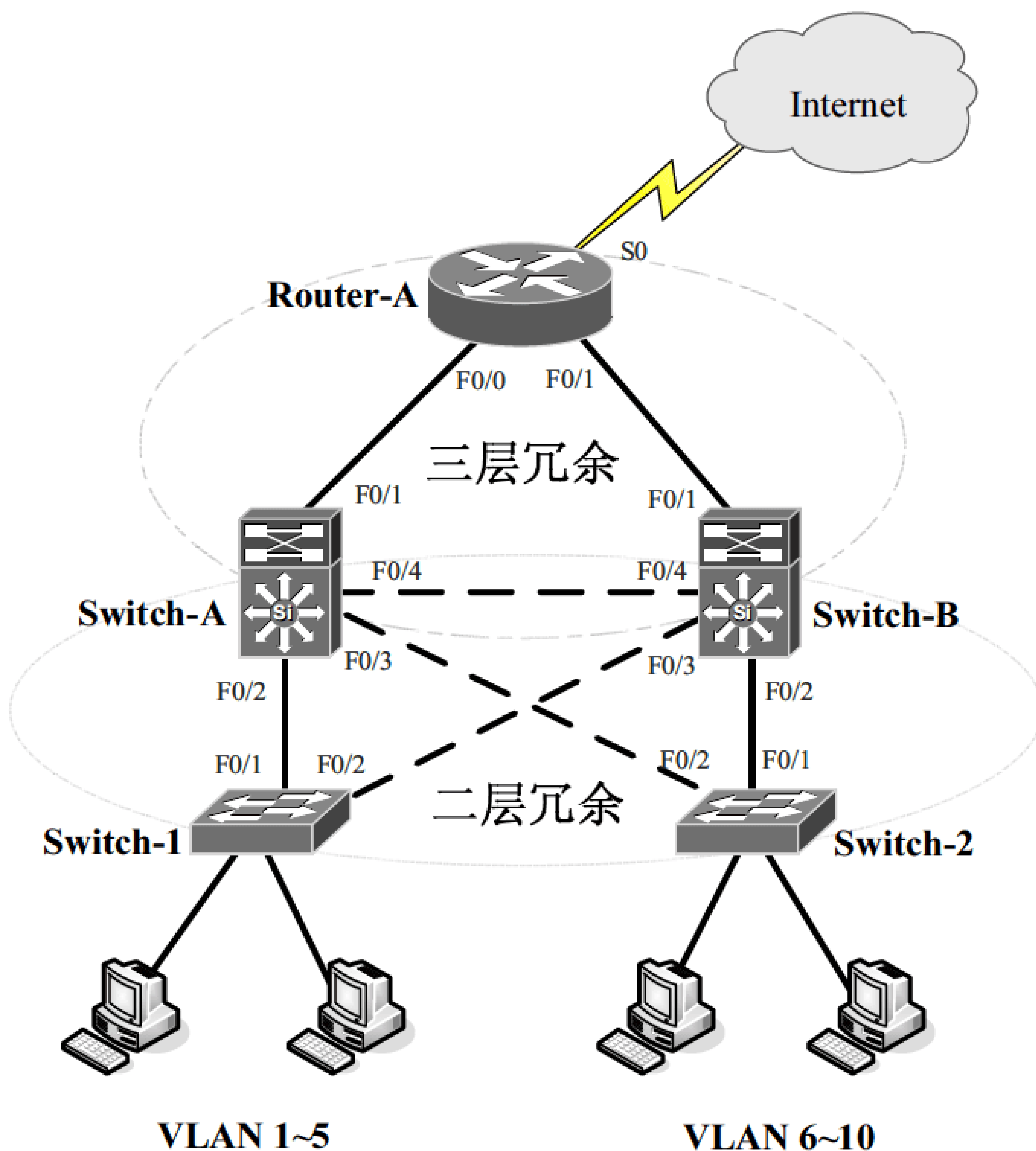


图 3-7 基于 VLAN 的多层冗余实验拓扑图

图 3-7 中两个三层交换机作为网络的双核心互做备份，并实现网络负载均衡。实例中配置 VLAN1~10，其中 VLAN1~5 以左侧链路为主进行通信，VLAN6~10 以右侧链路为主进行通信。即 Switch-A 为 VLAN1~5 的根桥和访问其他网络的网关，而 Switch-B 为 VLAN6~10 的根桥和访问其他网络的网关。表 3-2 为地址分配表。

表 3-2 地址分配表

Router-A	Switch-A	Switch-B
F0/0:192.168.100.1/24 F0/1:192.168.200.1/24	F0/1:192.168.100.2/24 VLAN1:192.168.1.252/24 VLAN2:192.168.2.252/24 VLAN3:192.168.3.252/24 …… VLAN9:192.168.9.252/24 VLAN10:192.168.10.252/24	F0/1:192.168.200.2/24 VLAN1:192.168.1.253/24 VLAN2:192.168.2.253/24 VLAN3:192.168.3.253/24 …… VLAN9:192.168.9.253/24 VLAN10:192.168.10.253/24

2. 设备基本配置

设备基本配置包括设备名、各种口令、VTP、中继链路、VLAN 的划分等，具体操作步骤如下。

01 初始化设备，为设备命名、配置口令等,，操作命令如下。

Switch-A：

```
Switch (config)#hostname Switch-A   //为设备命名
Switch-A (config)#enable secret Cisco    //为设备配置特权模式密文密码
Switch-A (config)#line console 0    //进入 console 口配置子模式
Switch-A (config-line)#login   //开启 console 加密登录功能
Switch-A (config-line)#password Cisco    //配置 console 口登录密码
Switch-A (config)#line vty 0 15    //进入 telnet 虚拟接口配置子模式
Switch-A (config-line)# login
Switch-A (config-line)#password Cisco
```

Switch-B：

```
Switch (config)#hostname Switch-B
Switch-B (config)#enable secret Cisco
Switch-B (config)#line console 0
Switch-B (config-line)#login
Switch-B (config-line)#password Cisco
Switch-B (config)#line vty 0 15
Switch-B (config-line)# login
Switch-B (config-line)#password Cisco
```

Switch-1：

```
Switch (config)#hostname Switch-1
Switch-1 (config)#enable secret Cisco
Switch-1 (config)#line console 0
Switch-1 (config-line)#login
Switch-1 (config-line)#password Cisco
Switch-1 (config)#line vty 0 15
Switch-1 (config-line)# login
Switch-1 (config-line)#password Cisco
```

Switch-2：

```
Switch (config)#hostname Switch-2
```

```
Switch-2 (config)#enable secret Cisco
Switch-2 (config)#line console 0
Switch-2 (config-line)#login
Switch-2 (config-line)#password Cisco
Switch-2 (config)#line vty 0 15
Switch-2 (config-line)# login
Switch-2 (config-line)#password Cisco
```

Router-A：

```
Router(config)#hostname Router-A
Router-A (config)#enable secret Cisco
Router-A (config)#line console 0
Router-A (config-line)#login
Router-A (config-line)#password Cisco
Router-A (config)#line vty 0 15
Router-A (config-line)# login
Router-A (config-line)#password Cisco
```

02 在 Switch-A 上创建 VLAN2~10，具体操作命令如下。

```
Switch-A#VLAN database
Switch-A(VLAN)#VLAN 1
VLAN 1 modified:
Switch-A(VLAN)#VLAN 2
VLAN 2 added:
    Name: VLAN0002
Switch-A(VLAN)#VLAN 3
VLAN 3 added:
    Name: VLAN0003
……
Switch-A(VLAN)#VLAN 10
VLAN 10 added:
    Name: VLAN0010
```

03 在四台交换机上分别配置 VTP 协议，将 Switch-A 和 Switch-B 配置为 VTP 服务器模式，Switch-1 和 Switch-2 作为客户端，具体操作命令如下。

Switch-A：

```
Switch-A(VLAN)#vtp domain Cisco     //指定 VTP 域，处于同一个 VTP 域的交换机才能交换、学习 VLAN 信息
Switch-A(VLAN)#vtp server           //指定该交换机为服务器模式
Switch-A(VLAN)#vtp v2-mode          //指定 VTP 版本号
Switch-A(VLAN)#vtp password Cisco   //配置 VTP 密码，用于认证
```

Switch-B：

```
Switch-B#VLAN database
Switch-B(VLAN)#vtp domain Cisco
Switch-B(VLAN)#vtp v2-mode
Switch-B(VLAN)#vtp server
Switch-B(VLAN)#vtp password Cisco
```

Switch-1：

```
Switch-1#VLAN database
Switch-1(VLAN)#vtp domain Cisco
Switch-1(VLAN)#vtp client              //指定交换机为客户端模式
Switch-1(VLAN)#vtp v2-mode
Switch-1(VLAN)#vtp password Cisco
```

Switch-2：

```
Switch-2#VLAN database
Switch-2(VLAN)#vtp domain Cisco
Switch-2(VLAN)#vtp client
Switch-2(VLAN)#vtp v2-mode
Switch-2(VLAN)#vtp password Cisco
```

04 因为 VTP 信息只在 trunk 接口上发送，所以交换机相连的接口需要配置成 trunk 接口，操作命令如下。

Switch-A：

```
Switch-A(config)#int f0/2
Switch-A(config-if)#switchport mode trunk
Switch-A(config)#int f0/3
Switch-A(config-if)#switchport mode trunk
Switch-A(config)#int f0/4
Switch-A(config-if)#switchport mode trunk
```

Switch-B：

```
Switch-B(config)#int f0/2
Switch-B(config-if)#switchport mode trunk
Switch-B(config)#int f0/3
Switch-B(config-if)#switchport mode trunk
Switch-B(config)#int f0/4
Switch-B(config-if)#switchport mode trunk
```

Switch-1：

```
Switch-1(config)#int f0/1
Switch-1(config-if)#switchport mode trunk
Switch-1(config)#int f0/2
Switch-1(config-if)#switchport mode trunk
```

Switch-2：

```
Switch-2(config)#int f0/1
Switch-2(config-if)#switchport mode trunk
Switch-2(config)#int f0/2
Switch-2(config-if)#switchport mode trunk
```

3. 二层链路冗余

二层链路冗余主要是使用 STP 生成树协议。依照实例中网络拓扑图的连接方法已经构成了二

层环路，链路冗余已经产生，但是其中关键的是哪些设备作为 STP 生成树协议的根桥。由于核心交换机的性能比较高，一般需要将两台核心交换机定义为根桥。

在实例中，有 10 个 VLAN，为了实现负载，需要让 Switch-A 作为 VLAN1~5 的根桥，Switch-B 作为 VLAN6~10 的根桥。为了确保其中一台核心交换机损坏后，根桥身份不被底层的低端交换机抢占，需要让 Switch-B 作为 VLAN1~5 的备用根桥，Switch-A 作为 VLAN6~10 的备用根桥。具体操作命令如下。

Switch-A：

```
Switch-A(config)#spanning-tree VLAN 1~5 priority 4096
//降低交换机 Switch-A 中 VLAN1~5 的优先级为 4096，确保其在 VLAN1~5 中的根桥身份
Switch-A(config)#spanning-tree VLAN 6~10 priority 8192
//降低交换机 Switch-A 中 VLAN6~10 的优先级为 8192，确保其在 VLAN6~10 中的备用根桥身份
```

Switch-B：

```
Switch-B(config)#spanning-tree VLAN 6~10 priority 4096
//降低交换机 Switch-B 中 VLAN6~10 的优先级为 4096，确保其在 VLAN6~10 中的根桥身份
Switch-B(config)#spanning-tree VLAN 1~5 priority 8192
//降低交换机 Switch-B 中 VLAN1~5 的优先级为 8192，确保其在 VLAN1~5 中的备用根桥身份
```

4. 三层链路冗余

三层链路冗余主要是用作网关备份，在配置冗余之前首先要确保网络访问畅通，所以要正确配置接口 IP 地址，并且要合适配置路由。在配置三层链路冗余时，主要使用 VRRP 协议，每一个 VLAN 作为一个 VRRP 组进行配置。

配置中除了要实现三层链路冗余外，还应该考虑网络负载均衡的问题，所以案例中将 Switch-A 作为 VLAN1-5 的 VRRP 主路由器，而 Switch-B 作为 VLAN6-10 的 VRRP 主路由器。

为双核心三层交换机的 VLAN 配置 VRRP 协议的具体配置方法如下。

01 为路由器、两台三层交换机的 VLAN 配置 IP 地址，具体操作命令如下。

Router-A：

```
Router-A(config)#interface f0/0
Router-A(config-if)#ip address 192.168.100.1 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config-if)#interface f0/1
Router-A(config-if)#ip address 192.168.200.1 255.255.255.0
Router-A(config-if)#no shut
```

Switch-A：

```
Switch-A(config)#interface f0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip address 192.168.100.2 255.255.255.0
Switch-A(config)#interface VLAN 1
Switch-A(config-if)#ip address 192.168.1.252 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config)#interface VLAN 2
Switch-A(config-if)#ip address 192.168.2.252 255.255.255.0
```

```
Switch-A(config-if)#no shut
Switch-A(config)#interface VLAN 3
Switch-A(config-if)#ip address 192.168.3.252 255.255.255.0
Switch-A(config-if)#no shut
……                                        //省略 VLAN4-8 的 IP 地址配置命令
Switch-A(config)#interface VLAN 9
Switch-A(config-if)#ip address 192.168.9.252 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config)#interface VLAN 10
Switch-A(config-if)#ip address 192.168.10.252 255.255.255.0
Switch-A(config-if)#no shut
```

Switch-B：

```
Switch-B(config)#interface f0/1
Switch-B(config-if)#no switchport
Switch-B(config-if)#ip address 192.168.200.2 255.255.255.0
Switch-B(config)#interface VLAN 1
Switch-B(config-if)#ip address 192.168.1.253 255.255.255.0
Switch-B(config-if)#no shut
Switch-B(config)#interface VLAN 2
Switch-B(config-if)#ip address 192.168.2.253 255.255.255.0
Switch-B(config-if)#no shut
Switch-B(config)#interface VLAN 3
Switch-B(config-if)#ip address 192.168.3.253 255.255.255.0
Switch-B(config-if)#no shut
……                                        //省略 VLAN4-8 的 IP 地址配置命令
Switch-B(config)#interface VLAN 9
Switch-B(config-if)#ip address 192.168.9.253 255.255.255.0
Switch-B(config-if)#no shut
Switch-B(config)#interface VLAN 10
Switch-B(config-if)#ip address 192.168.10.253 255.255.255.0
Switch-B(config-if)#no shut
```

02 为了确保内网客户端可以访问外网，需要沿网络出方向配置默认路由，本实例只有三台设备需要配置默认路由，操作命令如下。

Router-A：

```
Router-A(config)#ip route 0.0.0.0 0.0.0.0 S0    //配置默认路由，从 S0 口转出
```

Switch-A：

```
Switch-A(config)#ip route 0.0.0.0 0.0.0.0 f0/1
```

Switch-B：

```
Switch-B(config)#ip route 0.0.0.0 0.0.0.0 f0/1
```

03 在两台核心交换机上配置 VRRP 冗余，每一个 VLAN 都需要做网关冗余，所以需要对每一个 VLAN 做 VRRP 冗余配置，具体配置命令如下。

Switch-A：

```
Switch-A(config)#track 100 interface F0/1 line-protocol
//开启路由器端口跟踪，当三层交换机上端链路故障时，可通过接口 F0/1 的跟踪功能判断整条链路故障，
//从而使 VRRP 主路由器身份跳转
Switch-A(config-track)#exit
Switch-A(config)#int VLAN 1
Switch-A(config-if)#vrrp 1 ip 192.168.1.254
//在 VLAN1 中配置 VRRP 组 1，并制定虚拟路由器的 IP 地址为 192.168.1.254
Switch-A(config-if)#vrrp 1 priority 120
//修改 Switch-A 中 VRRP 组 1 的优先级为 120，以及在 VLAN1 中交换机 Switch-A 为主路由器
Switch-A(config-if)#vrrp 1 preempt
//开启抢占功能，交换机因故障丢失 VRRP 主路由器身份，为了确保该交换机故障修复后能够重新获得
//主路由器身份，必须开启抢占功能
Switch-A(config-if)#vrrp 1 authentication md5 key-string Cisco
//配置 VRRP 协议加密认证
Switch-A(config-if)#vrrp 1 track 100 decrement 30
//端口跟踪，发现链路故障时，自动将优先级降低 30，以便其他可用链路的设备抢夺 VRRP 主路由器身份
Switch-A(config)#int VLAN 2
Switch-A(config-if)#vrrp 2 ip 192.168.2.254
Switch-A(config-if)#vrrp 2 priority 120
Switch-A(config-if)#vrrp 2 preempt
Switch-A(config-if)#vrrp 2 authentication md5 key-string Cisco
Switch-A(config-if)#vrrp 2 track 100 decrement 30
Switch-A(config)#int VLAN 3
Switch-A(config-if)#vrrp 3 ip 192.168.3.254
Switch-A(config-if)#vrrp 3 priority 120
Switch-A(config-if)#vrrp 3 preempt
Switch-A(config-if)#vrrp 3 authentication md5 key-string Cisco
Switch-A(config-if)#vrrp 3 track 100 decrement 30
Switch-A(config)#int VLAN 4
Switch-A(config-if)#vrrp 4 ip 192.168.4.254
Switch-A(config-if)#vrrp 4 priority 120
Switch-A(config-if)#vrrp 4 preempt
Switch-A(config-if)#vrrp 4 authentication md5 key-string Cisco
Switch-A(config-if)#vrrp 4 track 100 decrement 30
Switch-A(config)#int VLAN 5
Switch-A(config-if)#vrrp 5 ip 192.168.5.254
Switch-A(config-if)#vrrp 5 priority 120
Switch-A(config-if)#vrrp 5 preempt
Switch-A(config-if)#vrrp 5 authentication md5 key-string Cisco
Switch-A(config-if)#vrrp 5 track 100 decrement 30

Switch-A(config)#int VLAN 6
Switch-A(config-if)#vrrp 6 ip 192.168.6.254
Switch-A(config-if)#vrrp 6 preempt
Switch-A(config-if)#vrrp 6 authentication md5 key-string Cisco
Switch-A(config)#int VLAN 7
Switch-A(config-if)#vrrp 7 ip 192.168.7.254
Switch-A(config-if)#vrrp 7 preempt
Switch-A(config-if)#vrrp 7 authentication md5 key-string Cisco
Switch-A(config)#int VLAN 8
```

```
Switch-A(config-if)#vrrp 8 ip 192.168.8.254
Switch-A(config-if)#vrrp 8 preempt
Switch-A(config-if)#vrrp 8 authentication md5 key-string Cisco
Switch-A(config)#int VLAN 9
Switch-A(config-if)#vrrp 9 ip 192.168.9.254
Switch-A(config-if)#vrrp 9 preempt
Switch-A(config-if)#vrrp 9 authentication md5 key-string Cisco
Switch-A(config)#int VLAN 10
Switch-A(config-if)#vrrp 10 ip 192.168.10.254
Switch-A(config-if)#vrrp 10 preempt
Switch-A(config-if)#vrrp 10 authentication md5 key-string Cisco
```

Switch-B：

```
Switch-B(config)#track 100 interface F0/1 line-protocol
Switch-B(config)#int   VLAN1
Switch-B(config-if)#vrrp 1 ip 192.168.1.254
Switch-B(config-if)#vrrp 1 preempt
Switch-B(config-if)#vrrp 1 authentication md5 key-string Cisco
Switch-B (config)#int VLAN 2
Switch-B(config-if)#vrrp 2 ip 192.168.2.254
Switch-B(config-if)#vrrp 2 preempt
Switch-B(config-if)#vrrp 2 authentication md5 key-string Cisco
Switch-B(config)#int VLAN 3
Switch-B(config-if)#vrrp 3 ip 192.168.3.254
Switch-B(config-if)#vrrp 3 preempt
Switch-B(config-if)#vrrp 3 authentication md5 key-string Cisco
Switch-B(config)#int VLAN 4
Switch-B(config-if)#vrrp 4 ip 192.168.4.254
Switch-B(config-if)#vrrp 4 preempt
Switch-B(config-if)#vrrp 4 authentication md5 key-string Cisco
Switch-B(config)#int VLAN 5
Switch-B(config-if)#vrrp 5 ip 192.168.5.254
Switch-B(config-if)#vrrp 5 preempt
Switch-B(config-if)#vrrp 5 authentication md5 key-string Cisco

Switch-B(config)#int VLAN 6
Switch-B(config-if)#vrrp 6 ip 192.168.6.254
Switch-B(config-if)#vrrp 6 priority 120
Switch-B(config-if)#vrrp 6 preempt
Switch-B(config-if)#vrrp 6 authentication md5 key-string Cisco
Switch-B(config-if)#vrrp 6 track 100 decrement 30
Switch-B(config)#int VLAN 7
Switch-B(config-if)#vrrp 7 ip 192.168.7.254
Switch-B(config-if)#vrrp 7 priority 120
Switch-B(config-if)#vrrp 7 preempt
Switch-B(config-if)#vrrp 7 authentication md5 key-string Cisco
Switch-B(config-if)#vrrp 7 track 100 decrement 30
Switch-B(config)#int VLAN 8
Switch-B(config-if)#vrrp 8 ip 192.168.8.254
Switch-B(config-if)#vrrp 8 priority 120
```

```
Switch-B(config-if)#vrrp 8 preempt
Switch-B(config-if)#vrrp 8 authentication md5 key-string Cisco
Switch-B(config-if)#vrrp 8 track 100 decrement 30
Switch-B(config)#int VLAN 9
Switch-B(config-if)#vrrp 9 ip 192.168.9.254
Switch-B(config-if)#vrrp 9 priority 120
Switch-B(config-if)#vrrp 9 preempt
Switch-B(config-if)#vrrp 9 authentication md5 key-string Cisco
Switch-B(config-if)#vrrp 9 track 100 decrement 30
Switch-B(config)#int VLAN 10
Switch-B(config-if)#vrrp 10 ip 192.168.10.254
Switch-B(config-if)#vrrp 10 priority 120
Switch-B(config-if)#vrrp 10 preempt
Switch-B(config-if)#vrrp 10 authentication md5 key-string Cisco
Switch-B(config-if)#vrrp 10 track 100 decrement 30
```

3.3 如何解决链路带宽不足

互联网发展速度迅猛，企业对于网络的性能、网速和带宽的要求日益增加，在这样的网络扩充中难免会出现链路带宽不足的现象。对于企业来说，解决链路带宽不足可以使用多种方法进行解决，下面分别进行介绍。

3.3.1 升级网络至千兆网络环境

100M 网络从出现至今已经有很长一段时间了，特别是前几年网络发展较迅猛的一段时间里，各个公司大都构建了 100M 网络环境随着技术的发展千兆网络技术已经完全成熟，而且最新搭建的网络大都是千兆网络环境，所以解决网络链路带宽不足的方法之一就是将百兆网络升级为千兆网络。

由 100M 网络升级为千兆网络不单单是要更换千兆线缆。以往的设备大都不是千兆接口，一旦更换为千兆网络，可能很多设备都需要更换。

所以，在将网络升级为千兆网络时，需要结合企业的经济状况和业务需求综合考虑。如果业务需求不那么迫切，可以先更换关键链路为千兆网络。

3.3.2 增加链路数量

当网络链路带宽不足时，可以将关键设备间的链路数量增加，一般都是一条链路连接两个设备，可以增加 2 条以上的链路同时通信。如两台核心交换机使用一条 100M 双绞线互联的话，借着交换机比较多的优势可以在两台交换机之间多连接几条 100M 的双绞线。

但是直接在交换机之间连接多条线缆的话可能会造成环路，导致广播风暴。所以在连接的同时还要使用相应的技术限制环路产生。那么这里一般使用的技术被称作以太网信道或者端口聚合。

以太网信道技术是比较流行的用来增加网络链路带宽的方法。使用该技术时首先需要两端设备都支持以太网信道技术，同时进行端口捆绑的多个接口的状态要相同，如带宽、速度、双工模式

等，最好用连排的几个接口。

3.3.3 项目实战 3：使用以太网信道（端口聚合）增加主干链路带宽

使用以太网信道技术增加主干链路带宽的操作方法如下。

1. 实验拓扑

可依照图 3-8 所示网络拓扑图进行实验。

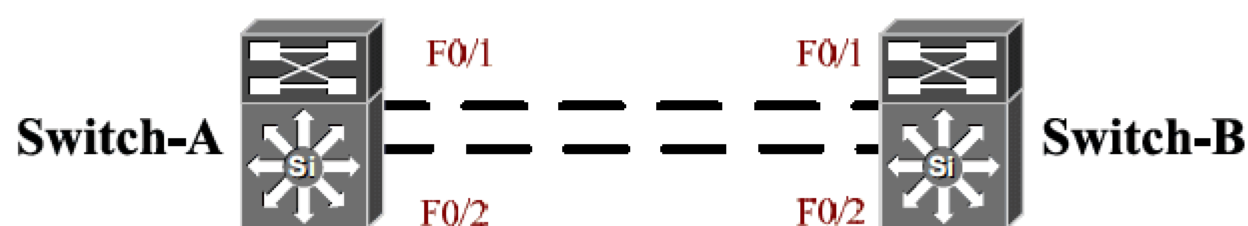


图 3-8 以太网信道实验拓扑

网络拓扑图中显示为两台核心交换机互连，使用两条 100M 全双工以太网链路进行端口聚合，聚合后可构成一条 200M 全双工的链路。

2. 项目配置

01 由于两台核心交换机之间会传输多个 VLAN 的数据，所以进行端口聚合的链路必须是 trunk 链路，所以交换机相连的接口需要配置成 trunk 接口，操作命令如下。

Switch-A：

```
Switch-A(config)#int f0/1
Switch-A(config-if)#switchport mode trunk
Switch-A(config)#int f0/2
Switch-A(config-if)#switchport mode trunk
```

Switch-B：

```
Switch-B(config)#int f0/1
Switch-B(config-if)#switchport mode trunk
Switch-B(config)#int f0/2
Switch-B(config-if)#switchport mode trunk
```

02 进行端口聚合需要将多个接口组合成一个逻辑信道，操作命令如下。

Switch-A:

```
Switch-A(config)#interface range fastethernet0/1 - 2
//进入 F0/1 和 F0/2 的配置子模式
Switch-A(config-if-range)#channel-group 1 mode on
//将 F0/1 和 F0/2 组合为逻辑信道“channel-group 1”
```

Switch-B：

```
Switch-B(config)#interface range fastethernet0/1 - 2
//进入 F0/1 和 F0/2 的配置子模式
Switch-B(config-if-range)#channel-group 1 mode on
//将 F0/1 和 F0/2 组合为逻辑信道“channel-group 1”
```

03 使用 show etherchannel summary 命令检查快速以太网通道连接状况。

```
Switch#show etherchannel summary
Flags:  D - down            P - in port-channel
         I - stand-alone s - suspended
         H - Hot-standby (LACP only)
         R - Layer3          S - Layer2
         U - in use          f - failed to allocate aggregator
         u - unsuitable for bundling
         w - waiting to be aggregated
         d - default port


Number of channel-groups in use: 1
Number of aggregators:               1

Group  Port-channel  Protocol    Ports
------+------------+----------+-------------------------------------------

1        Po1(SU)             PAgP    Fa0/1(P) Fa0/2(P)
```



提 示

在使用以太网信道时，最多支持 8 条快速以太网接口聚合。

3.4 网络流量控制

网络畅通是网络搭建中必要的要求，但是并非所有的网络流量都应该被转发的，为了安全，为了满足部分业务流量的优先服务要求，总是有一些流量需要被限制。常用的网络流量控制技术有访问控制列表和服务质量，具体内容介绍如下。

3.4.1 访问控制列表

访问控制列表（ACL）的具体内容介绍如下。

1. ACL 概述

ACL 是最常用的网络流量限制技术，通过该技术可以为路由器或交换机的接口配置一些控制指令，用来控制接口的进出数据包。ACL 可配置禁止或允许指定流量通过，流量可通过 ACL 本身的配置进行筛选，比如在指定接口筛选接收的 FTP 请求。

2. ACL 的配置方法

配置 ACL 主要有两个步骤，首先要指定访问控制条件，需要创建列表编号或名称，然后在指定列表编号或名称内添加流量筛选条件，并指定是允许（permit）或拒绝（deny）。如“router(config)#access-list 10 deny 3.3.3.0 0.0.0.255”，在编号为 10 的访问控制列表中禁止来自

3.3.3.0/24 网段的流量，其中“0.0.0.255”为反子网掩码。

配置完 ACL 访问控制列表后，需要将其指定在某个接口进行应用，如“router(config-if)#ip access-group 10 in”，在路由器 F1/1 接口流入方向应用访问控制列表 10，其中 in 表示流入方向，也可以使用 out 限制流出方向的数据。

配置访问控制列表时，应注意以下几点。

（1）访问列表的编号指明了使用何种类型的访问列表。

（2）每个端口、每个方向、每条协议只能对应于一个访问列表。

（3）访问列表的内容决定了数据的控制顺序。

（4）具有严格限制条件的语句应放在访问列表所有语句的最上面。

（5）在访问列表的最后有一条隐含声明：deny any，禁止所有流量。所以每一条正确的访问列表都至少应该有一条允许语句。

（6）先创建访问列表，然后应用到端口上。

（7）访问列表不能过滤由路由器自己产生的数据。

（8）在接口上应用空的 ACL，默认情况下允许所有流量。

3. ACL 的分类

访问控制列表根据筛选条件不同，可以分为标准访问控制列表、扩展访问控制列表、命名访问控制列表和定时访问控制列表。

（1）标准访问控制列表只可以限制指定源地址的流量，通常使用 1~99 的列表编号。使用标准访问控制列表，一旦有一个访问控制条目匹配，后面的控制条目不再查看。

例：

① 阻止 IP 地址 172.16.4.13 发送的数据，特定主机为源地址的话也可以配置为“host 172.16.4.13”。

```
Router(config)#access-list 1 deny 172.16.4.13 0.0.0.0
```

② 允许 172.16.0.0/24 网段主机发送的数据。

```
Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255
```

③ 允许所有流量，默认每一个列表编号最后都有一个隐藏的禁止所有流量的条目，如果不需要禁止其他所有流量，则需要配置该条目做补充，也可以使用 any 表示所有流量。

```
Router (config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

或

```
Router (config)#access-list 1 permit any
```

（2）扩展访问控制列表可以针对源地址、目标地址、传输层协议、源端口、目标端口等进行流量控制，通常使用 100~199 的列表编号。使用时每个条件都必须匹配了才会拒绝或允许转发。

例：

① 拒绝来自 172.16.4.0，去往 172.16.3.0 的 ftp 流量。“eq”表示等于，用于指定特定端口。

```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Router(config)#access-list 101 permit ip any any
```

② 拒绝来自 172.16.4.0，去往 172.16.3.0 的 telnet 流量。

```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23
Router(config)#access-list 101 permit ip any any
```

（3）命名访问控制列表不使用列表编号，可以为访问控制列表指定具有特殊意义的名字。命名的访问控制列表中还可以分为标准和扩展两种，standard 表示标准，extended 表示扩展。

例：创建名为 Cisco 的命名访问控制列表，拒绝从 172.16.4.0/24 到 172.16.3.0/24 的 telnet 访问，并应用在设备的 E0 出口方向。

01 创建名为 Cisco 的命名访问控制列表，需要限制到 telnet 协议，所以采用扩展访问控制列表。

```
Router(config)#ip access-list extended Cisco
```

02 添加访问控制条件，加上允许其他所有流量。

```
Router(config-ext-nacl)# deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23
Router(config-ext-nacl)# permit ip any any
```

03 应用到接口 E0 的出口方向。

```
Router(config)#interface fastethernet 0/0
Router(config-if)#ip access-group Cisco out
```

（4）定时访问控制列表，可以按照一定的计划任务执行流量控制。

例：路由器的管理地址为 10.1.1.1，只允许远程客户端 20.1.1.1 在 2010 年 11 月 1 日至 2012 年 6 月 30 日的每周一到周五的 8：00 到 18：00 和周末的 9：00 到 21：00 进行 telnet 登录。

01 创建访问控制的时间范围。

```
Router(config)#time-range telnettime //定义时间范围名
Router(config-time-range)#absolute start 00:00 1 nov 2010 end 00:00 1 jun 2012    //定制访问控制的时间跨度范围为 2010. 11. 1-2012. 6. 30
Router(config-time-range)#periodic  weekday  08:00  to  18:00   //定制周期性执行时间为工作日的  18:00-18:00，weekday 表示工作日周一到周五
Router(config-time-range)#periodic  weekend  09:00  to  21:00    //定制周期性执行时间为周末的  09:00-21:00，weekend 表示周六和周日
Router(config-time-range)#exit
```

02 创建扩展访问控制列表，应用访问控制时间，并定义流量筛选条件。

```
Router(config)#access-list 110 permit tcp host 20.1.1.1 host 10.1.1.1 eq 23 time-range telnettime
```

03 在路由器 S0 口的进入方向应用访问控制列表。

```
Router(config)#int S0
Router(config-if)#ip access-group 110 in
```

3.4.2　服务质量

服务质量（QoS）的具体内容介绍如下。

1. QoS 概述

QoS 是网络的一种安全机制，用来解决网络延迟和阻塞等问题的重要技术。通常情况下，如果网络只用于没有时间限制的应用系统，并不需要 QoS 技术，如 Web 应用、E-Mail 等。但是对于对网络带宽速率要求比较高的应用，如流媒体访问、视频会议等，就十分必要。当网络过载或出现拥塞时，使用 QoS 协议可以确保重要业务优先转发，减少延迟和丢弃现象，同时也可以提高网络利用效率。

2. QoS 的工作模式

QoS 主要有三种工作方式，分别介绍如下。

（1）Best-Effort service（尽力而为的服务模型）：先进先出的转发方式，按照数据包的接收顺序进行转发。这也是网络中默认的数据转发方式，不能对网络中的重要业务流进行优先转发操作。

（2）Integrated service（综合服务模型）：提前为重要数据流申请网络资源，为各节点预留资源，如分配 1M 的独立带宽供其使用。这种方法可以有效地保证重要业务流的传输，但是当重要业务流传输结束或暂停时，申请的网络资源不能够释放，只能空闲等待，这样不利于网络资源的充分利用。

（3）Differentiated service（区分服务模型）：不预留资源，将流量进行分类，通过流量对网络性能的要求配置转发级别，只要有需要优先转发的数据，永远会优先处理。这种方式可以更高效地利用网络资源，使用比较普遍。

QoS 的工作主要由三步来完成：

（1）标识流量类型及其需求，也就是指定现实网络中需要对哪些流量进行 QoS 操作。
（2）基于所标识的需求信息进行流量分类，例如使用 ACL 将部分主机流量分离出来。
（3）为每种流量类别定义相关策略，即为不同流量指定优先转发级别。

3. QoS 的具体实现

QoS 一般可以使用队列的方式进行流量分流，并控制其优先转发级别，主要有优先级队列、自定义队列、基于类的加权公平队列、低延迟队列等多种方式。

（1）优先级队列(priority queue,PQ)：可将数据分为高、中、普通、低优先级 4 种队列，依次完成队列内容转发，当上级完成后方可进行低级队列内容。如果高级队列一直有数据传输，低级队列的数据可能很久也得不到转发，这样可以为每一个队列指定一个长度，当转发数据达到一定长度后，就必须降级转发低一级的队列数据。4 种级别的名称分别为 high、medium、normal 、low。

例：将经过路由器 Router-A 的流量按照优先级队列方式进行分流转发操作。

01 确定队列信息流，将信息流分入不同级别的队列中。

```
Router-A(config)#priority-list 1 protocol ip high tcp 23
```

```
//将 TCP 协议中 23 端口的 telnet 流量放入高级队列
Router-A (config)#priority-list 1 protocol ip high list 100
//将访问控制列表 100 的流量放入高级队列
Router-A (config)#priority-list 1 protocol ip medium tcp 80
//将 TCP 协议中的 80 端口的 Web 访问流量放入中级队列
Router-A (config)#priority-list 1 interface f0/1 normal
//将来自接口 F0/1 的流量放入普通级别队列
Router-A (config)#priority-list 1 default low
//将其余流量放入低优先级队列，这一命令不能省略，否则其他流量将无法被转发
```

02 在指定接口应用流量控制规则。

```
Router-A (config)#int s1/0
Router-A (config-if)#priority-group 1    //应用优先级队列 1
```

03 使用 show queueing 命令查看优先级队列 QoS 配置。

```
R1#show queueing
Current fair queue configuration:
  Interface          Discard    Dynamic   Reserved   Link     Priority
                     threshold  queues    queues     queues   queues
  Serial1/0          64         256       0          8        1
  Serial1/1          64         256       0          8        1

Current DLCI priority queue configuration:
Current priority queue configuration:
List   Queue   Args
1      high    protocol ip          tcp port 23
1      high    protocol ip          list 100
1      medium protocol ip           tcp port 80
1      low     default
```

（2）自定义队列(custom queue,CQ)：将数据包定义到 16 个不同的队列中，依次执行队列内数据包转发，每个队列一次只执行指定数量的数据包长度，队列“0”为空时才可转发其他队列数据包。

例：将经过路由器 Router-A 的流量按照自定义队列方式进行分流转发操作。

01 确定队列信息流，将信息流分入不同级别的队列中。

```
Router-A(config)#queue-list 1 protocol ip 1 tcp 23
//将 TCP 协议中 23 端口的 telnet 流量放入 1 号队列
Router-A (config)#queue-list 1 protocol ip 2 list 100
//将访问控制列表 100 的流量放入 2 号队列
Router-A (config)#queue-list 1 protocol ip 3 gt 1000
//将大于 1000 字节的数据包放入 3 号队列
Router-A (config)#queue-list 1 interface f0/1 5
//将来自 F0/1 接口的流量放入 5 号队列
Router-A (config)#queue-list 1 default 6
//将其他数据流放入 6 号队列，该命令不能省略
```

02 为每一个队列指定数据包深度，队列深度值越大，该级别的数据被转发的效率越高。

```
Router-A (config)#queue-list 1 queue 1 limit 40
```

```
Router-A (config)#queue-list 1 queue 2 limit 30
Router-A (config)#queue-list 1 queue 3 limit 20
Router-A (config)#queue-list 1 queue 5 limit 10
```

03 在指定接口应用自定义序列。

```
Router-A (config)#int s1/0
Router-A (config-if)#custom-queue-list 1
```

（3）基于类的加权公平队列(class based weight fair queue,CBWFQ)：允许用户自定义类别，通过制定类别的带宽控制其转发有限级别。

例：将经过路由器 Router-A 的流量按照基于类的加权公平队列方式进行分流转发操作。

01 定义流量区分表，将信息流分入不同的 class-map 队列表中。

```
Router-A(config)#class-map match-all class-map1
//自定义流量区分表的第一个队列 class-map 1
Router-A(config-cmap)#match protocol http
//将 http 协议流量放入 class-map 1 队列中
Router-A(config-cmap)#match input-interface f0/1
//将来自 F0/1 接口的流量放入 class-map 1 队列中
Router-A(config)#class-map match-any class-map2
//自定义流量区分表的第二个队列 class-map 2
Router-A(config-cmap)#match access-group 100
//将访问控制列表 100 定义的流量放入 class-map 2 队列中
Router-A(config-cmap)#match ip precedence critical
//匹配 IP 数据包的优先级，将优先级为 critical（紧急的）数据包放入 class-map2 队列中，每一个 IP 数据包都有 IP 优先级，一般可以根据数据包的数据类型产生不同的优先级，critical 只是其中之一
```

02 为每一个队列定义流量策略，一般使用带宽分配的方式指定其优先转发级别。

```
Router-A(config)#policy-map my-policy
//创建策略集 my-policy
Router-A(config-pmap)#class class-map1
//在策略集中为 class-map1 队列配置策略
Router-A(config-pmap-c)#bandwidth 60 （kbps）
//为队列 class-map1 指定 60kbps 的带宽，也可以使用“bandwidth percent 80”命令，为其分配总带宽的 80%
Router-A(config-pmap)#class class-map2
//在策略集中为 class-map1 队列配置策略
Router-A(config-pmap-c)#bandwidth 10
//为队列 class-map 2 指定 10kbps 的带宽
```

03 在指定接口启用流量策略。

```
Router-A(config)#int s0/0
Router-A(config-if)#service-policy output my-policy
//在接口 s0/0 的出口方向应用 my-policy 流量策略
```

（4）低延迟队列：可指定延迟敏感数据流，延迟敏感数据流传输完之前不传输其他类型数据。其配置方法和基于类的加权公平队列相似，这里就不再介绍。

3.4.3 项目实战 4：使用扩展访问控制列表确保 VLAN 间安全访问

在企业局域网中，访问控制列表配置是使用最普遍的技术，通常和 VLAN 结合使用。结合实际需求下面给出一个简单的企业网访问控制列表的配置案例。

1. 实验拓扑图

图 3-9 所示为模拟的网络拓扑结构，依此图进行案例介绍。

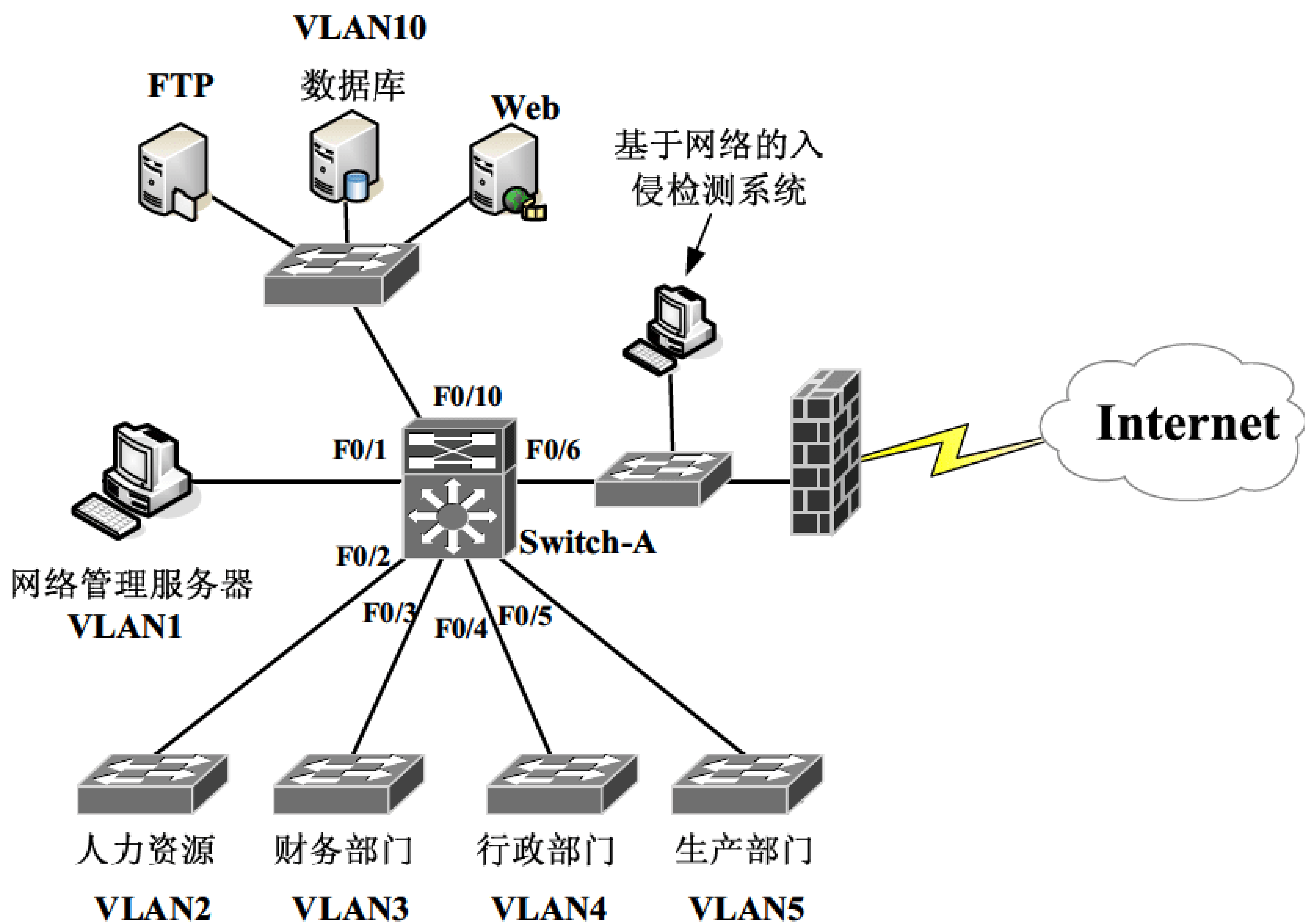


图 3-9 访问控制列表配置案例拓扑图

依照图 3-9 为网络规划地址配置，地址分配如表 3-3 所示。

表 3-3 网络规划地址配置

VLAN	IP 地址分配	设备	IP 地址分配
VLAN1（管理 VLAN）	192.168.100.0/24	网络管理服务器	192.168.100.10
VLAN2（人力资源部）	192.168.2.0/24	FTP 服务器	192.168.10.10
VLAN3（财务部门）	192.168.3.0/24	数据库服务器	192.168.10.20
VLAN4（行政部门）	192.168.4.0/24	Web 服务器	192.168.10.30
VLAN5（生产部门）	192.168.5.0/24	入侵检测服务器	192.168.1.100
VLAN10（内网服务器）	192.168.10.0/24		

2. 实验要求

在现实的网络结构中，需要配置以下访问控制规则。

（1）所有部门都允许访问企业 FTP 和 Web 服务器，只有财务部和生产部可以访问数据库服务器。

（2）网络管理员可以访问所有网络资源，并且只有网络管理员可以访问网络设备、入侵检测系统。

（3）为了财务部安全，限制财务部访问互联网。

（4）员工只能在周一至周五 08:00—18:00 和周末 08:00—12:00 这两个时间段访问互联网。

对于大型的校园网可能会有更复杂的配置要求，但是技术都相似，这里不再过多介绍。

3. 实验配置

可依照以下步骤完成实验配置。

01 在 Switch-A 上划分 VLAN，配置 IP 地址，此内容前面章节有详细介绍。

02 配置各个 VLAN 主机对内网服务器的访问权限。为了安全，建议只对客户端开放服务器的必要端口。

```
Switch-A(config)#access-list 101 permit ip host 192.168.100.10 any
//允许网络管理服务器访问内网服务器 VLAN 的所有主机
Switch-A(config)#access-list 101 permit tcp any host 192.168.10.10 eq ftp
//允许所有主机访问 FTP 服务器 192.168.10.10 的 ftp 端口
Switch-A(config)#access-list 101 permit tcp 192.168.3.0 0.0.0.255 host 192.168.10.20
//允许财务部网络 192.168.3.0/24 访问数据库服务器
Switch-A(config)#access-list 101 permit tcp any host 192.168.10.30 eq www
//允许所有主机访问 Web 服务器 192.168.10.30 的 WWW 服务端口
Switch-A(config)#access-list 101 deny any any
//该条为默认隐藏条目，可以不输入
Switch-A(config)#int VLAN 10
Switch-A(config-if)#ip access-group 101 in
//在 VLAN10 的入方向应用访问控制列表 101
```

03 禁止其他 VLAN 的主机访问网络设备和网络管理服务器。

```
Switch-A(config)#access-list 102 deny any any
Switch-A(config)#int VLAN 1
Switch-A(config-if)#ip access-group 102 in
```

04 设置员工互联网访问权限。

```
Switch-A (config)#time-range telnettime    //定义时间范围名
Switch-A (config-time-range)#periodic weekday 08:00 to 18:00
//定制周期性执行时间为工作日的 18:00-18:00
Switch-A (config-time-range)#periodic weekend 08:00 to 12:00
//定制周期性执行时间为周末的 08:00-12:00
Switch-A (config-time-range)#exit
Switch-A (config)#access-list 104 deny ip 192.168.3.0 0.0.0.255 any
//禁止财务部访问互联网
Switch-A (config)#access-list 104 permit tcp any any time-range telnettime
//创建扩展访问控制列表，应用访问控制时间，并定义流量筛选条件
```

05 在路由器 S0 口的进入方向应用访问控制列表。

```
Router(config)#int f0/6
Router(config-if)#ip access-group 104 out
//在接口 F0/6 的出方向应用访问控制列表 104
```

3.5 企业网络出口的 NAT+ACL 方案实现

由于企业内网大都使用私有地址，如果内网用户想要访问互联网，就必须使用 NAT 地址转换技术，将私有地址转换为在互联网应用的公有地址。在使用 NAT 技术时，往往使用 ACL 技术指定允许转换的内部主机地址范围。本节将详细介绍企业中 NAT+ACL 技术的应用。

3.5.1 NAT 地址转换技术概述

1. 为什么使用 NAT 技术

NAT 地址转换技术的提出是有现实背景的，首先合法的 IP 地址资源日益短缺，不可能为每一个主机都分配一个与众不同的 IP 地址，所以在局域网中一般都是用可以重复利用的私有地址。国际上规定 A、B、C 三类地址段分别有一部分私有地址段，A 类私有地址为 10.0.0.0~10.255.255.254，B 类私有地址段为 172.16.0.0~172.31.255.254，C 类私有地址段为 192.168.0.0~192.168.255.254。

私有地址只能在局域网中使用，不能出现在互联网，那么使用私有地址的内网主机想要访问互联网，就必须使用地址转换技术将其转换为公有地址。

使用 NAT 技术还有一个好处，内网的主机、服务器如果不对其做 NAT 技术，公共互联网用户就无法访问到它，所以 NAT 技术也可以对内网做到安全隔离的作用。

2. NAT 的原理

NAT 技术的工作原理很简单，即在出口设备上为每一个需要对外访问的主机的私有地址映射一个可用的公有地址，当数据包通过 NAT 设备时，改变其 IP 包头，使原有的目的地址、源地址或两个地址在包头中被新的映射地址替换。

根据映射的方式，可以将 NAT 技术分为 3 种实现方式：静态转换、动态转换、端口多路复用。

（1）静态 NAT：是手工配置的内部私有地址和外部公共地址的对应关系，除非手工修改，否则不会变化，一般对外发布服务器使用静态 NAT 技术。

（2）动态 NAT：是多个内部主机地址和外部公共地址随机对应的一种方式，主要通过指定内部允许转换的地址范围和外部允许使用的地址范围，然后对两个范围映射。这样具体外部的某一个公共地址被内部哪台主机使用不确定。主要适用于企业内网大量员工客户端访问外网。

（3）端口多路复用 NAT：又称作 PAT。由于可用的公共地址毕竟有限，如果让一个内部私有地址对应一个外部公有地址的话，并不能起到节省 IP 地址的作用，所以通常会考虑一个外部公共地址被内部多个私有 IP 地址共同使用。端口多路复用 NAT 就是很好的实现方法，它的 NAT 映射已经不再是简单的 IP 映射，而是细化到了端口映射，每一个 IP 都可以分化为多个端口。一个公共地址分出的每一个端口都可以映射内部的一个私有地址，这样就可以做到大大节约公有地址。这是目前企业局域网中使用最普遍的 NAT 技术。

3. NAT 的优点和缺点

通过以上内容的介绍，NAT 技术的优点可总结为以下几点。

（1）极大地节省了公有合法 IP 地址的使用。

（2）可以实现私有地址的交叉重复使用。

（3）局域网完全和互联网隔离，通过 NAT 技术可以灵活地限制、管理局域网上网的问题。

（4）互联网各种信息都有，存在有很多不安全因素，利用 NAT 技术隔离局域网，让局域网更安全。

NAT 技术的缺点可以总结为以下几点。

（1）由于 NAT 技术属于软件处理地址转换，会增加数据转发的延迟。

（2）NAT 技术为管理人员增加了很多配置和维护任务，对于大型网络 NAT 技术的复杂性较高。

（3）并非所有的技术都支持 NAT 转换，不过常规互联网访问应用都可以使用该技术。

3.5.2　项目实战 5：为企业对外发布服务器配置静态 NAT

企业内网服务器需要被外部用户访问，就必须对其做 NAT 转换，一般服务器要能够提供稳定、持续的访问，所以内部服务器映射的公共地址不能随意更换，需要使用静态 NAT 技术，下面来做一个案例。

1. 实验拓扑图

按照图 3-10 所示的网络拓扑图连接设备进行实验。

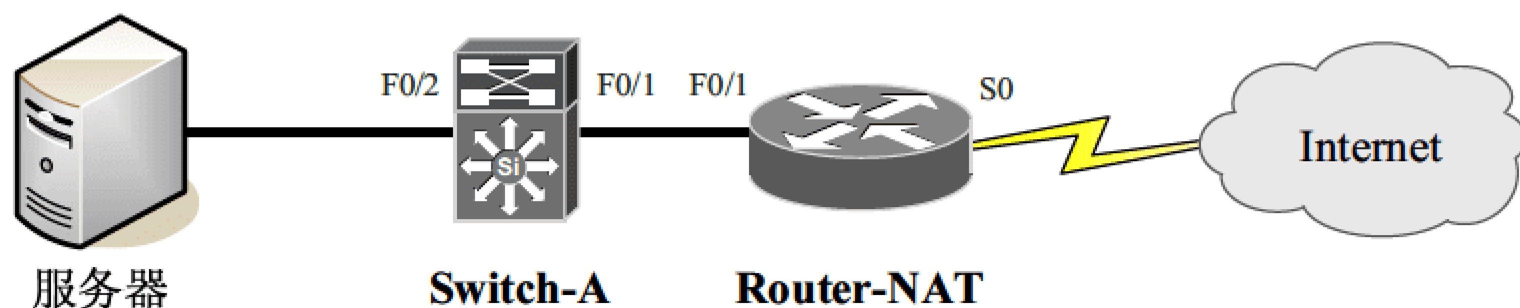


图 3-10　企业对外发布服务器的静态 NAT 拓扑图

依照图 3-10 为网络规划地址配置，地址分配如表 3-4 所示。

表 3-4　网络设备地址配置

设备	IP 地址分配
路由器	F0/1:192.168.1.1/24 S0:200.200.200.1
服务器	192.168.1.100/24

2. 实验配置

可依照以下步骤完成实验配置。

01　按图 3-10 所示网络拓扑图对网络设备做基础配置，包括设备命名、地址配置、设备加密等内容。这些内容前面小节中有介绍，这里不做演示。配置完成后要检验设备之间的连通性。

02　在 Router-NAT 上配置一条内网访问互联网的默认路由。

```
Router-NAT(config)#ip route 0.0.0.0 0.0.0.0 s0
```

03　为服务器配置静态 NAT 转换。

```
Router-NAT(config)#ip nat inside source static 192.168.1.100 200.200.200.2
//IP 地址 200.200.200.2 是从运营商申请的用于发布服务器的公共地址
```

04 指定 NAT 的内部接口和外部接口。

```
Router-NAT(config)#int f0/1
Router-NAT(config-if)#ip nat inside
Router-NAT(config)#int s0
Router-NAT(config-if)#ip nat outside
```

3.5.3 项目实战 6：为企业员工配置基于端口的动态地址转换技术 PAT

企业内网员工比较多，使用静态 NAT 为每一个员工配置一个映射地址很不现实，必须动态配置地址映射关系，以提高管理效率。使用动态的 NAT 技术虽然可以满足配置上的需求，但是显然不可能动态地为每个内部主机映射一个 IP 地址，需要使用细化端口的方式建立映射管理，确保一个 IP 地址可以分为多个端口供内部地址映射使用，这就要用到 PAT 技术了。下面详细介绍 PAT 技术的配置方法。

1. 实验拓扑图

按照图 3-11 所示网络拓扑图连接设备进行实验。

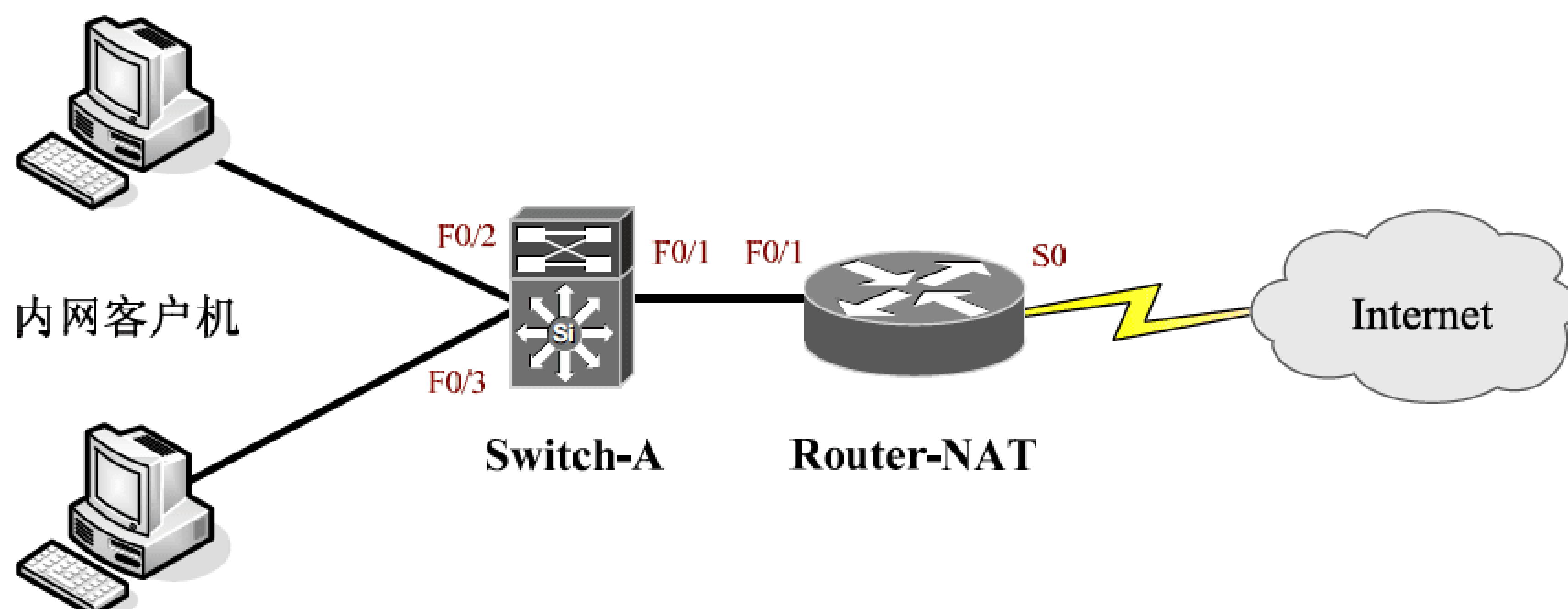


图 3-11 PAT 配置实验拓扑图

2. 实验配置

实现企业员工通过出口设备访问互联网的配置如下。

01 按图 3-11 所示网络拓扑图对网络设备做基础配置，包括设备命名、地址配置、设备加密等内容。

02 在 Router-NAT 上配置一条内网访问互联网的默认路由。

```
Router-NAT(config)#ip route 0.0.0.0 0.0.0.0 s0
```

03 创建一条定义了所有内部用户的标准的访问控制列表

```
Router-NAT(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

04 配置内部主机可以使用的公共 IP 地址池，如果只有一个地址，地址范围的起始地址和终止地址相同即可。

```
Router-NAT(config)#ip nat pool public 200.200.200.1 200.200.200.1 netmask 255.255.255.128
```

05 配置外网公共 IP 地址和内网可转换地址的映射关系，即外部公共 IP 地址池和内部指定访问控制列表的映射。

```
Router-NAT(cinfig)#ip nat inside source list 1 pool public
```

06 指定 NAT 的内部接口和外部接口。

```
Router-NAT(config)#int f0/1
Router-NAT(config-if)#ip nat inside
Router-NAT(config)#int s0
Router-NAT(config-if)#ip nat outside
```

可通过表 3-5 所示命令查看 NAT 转换的配置信息。

表 3-5　查看 NAT 转换的配置信息的命令

命令	功能
Router#show ip nat translations	显示 NAT 转换表
Router#show ip nat statistics	显示当前 NAT 状态
Router#clear ip nat translations*	在超时前清除所有 NAT 转换

3.5.4　项目实战 7：实现出口 NAT 的双线接入

目前最大的 Internet 服务提供商有两个，网通（联通）和电信。这两家网络运营商分别占用了一定的网络市场，普通家庭或企业用户可能存在于任何一家运营商的网络中，而两家运营商中的用户互通信息时并没有想象得那么快捷，需要经过两大运营商之间的跳转设备才可互通。这样一来，依靠互联网运营的企业就会受到很大影响了，特别是网络游戏和流媒体视频服务器。为了能够确保每一个运营商网络中的客户都可以高效地访问网络游戏服务器和流媒体服务器，这些企业有必要同时接入多个运营商网络。这种同时接入多个运营商网络的方式被称作出口 NAT 的双线接入（主要有联通和电信两大运营商）。

1. 实验网络拓扑图

按照图 3-12 所示网络拓扑图连接设备进行实验。

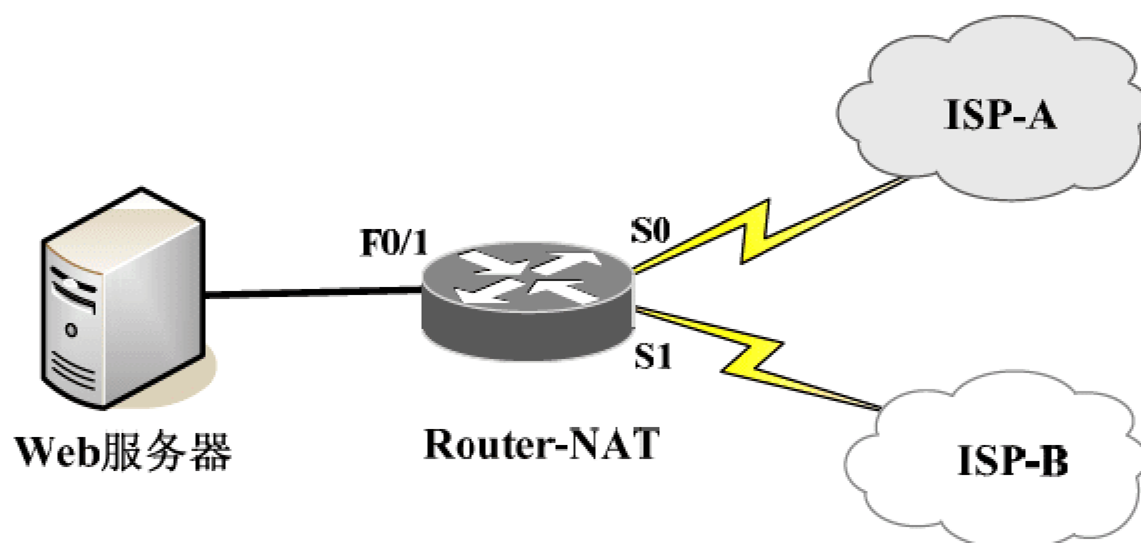


图 3-12　出口 NAT 双线接入网络拓扑图

依照图 3-12 为网络规划地址配置，地址分配如表 3-6 所示。

表 3-6 地址分配

设备	地址
Router-NAT	F0/1:192.168.1.1/24 S0:61.192.93.100/24 S1:202.102.100.100/24
Web 服务器	192.168.1.100/24
ISP-A	61.192.93.200/24
ISP-B	202.102.100.200/24

2. 实验配置

实现网络出口 NAT 双线接入的配置方法如下。

1）为网络出口路由器 Router-NAT 配置接口地址

为路由器配置接口地址的操作命令如下。

```
Router-NAT(config)#interface s0
Router-NAT(config-if)#ip add 61.192.93.100 255.255.255.0
Router-NAT(config-if)#no shutdown
Router-NAT(config)#interface s1
Router-NAT(config-if)#ip add 202.102.100.100 255.255.255.0
Router-NAT(config-if)#no shutdown
Router-NAT(config-if)#interface f0/1
Router-NAT(config-if)#ip address 192.168.1.1 255.255.255.0
Router-NAT(config-if)#no shutdown
```

2）为内网用户配置基于端口的动态 NAT 转换

内网用户访问互联网时，由于用户数量多，可用公网地址少，所以需要配置基于端口的动态 NAT 转换，即配置 PAT。具体配置步骤如下。

01 通过访问控制列表区分内网访问不同互联网运营商的数据流。

```
Router-NAT (config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
Router-NAT (config)#access-list 101 deny ip any 61.192.93.0 0.0.0.255
Router-NAT(config)#access-list 101 permit ip any any
```



提 示

需要配置两个访问控制列表来定义访问两个运营商的流量，其中 access-list 100 定义了到达 ISP-A 所有网段的 ACL，此处以 61.192.93.0/24 代表 ISP-A 所有网段。access-list 101 定义到达 ISP-B 所有网段的流量，用排除 ISP-A 网段的方式进行定义，可以防止遗漏网段。

02 为用户分别定义访问 ISP-A 和 ISP-B 的合法地址池。

```
Router-NAT(config)#ip nat pool ISP-A 61.192.93.100 61.192.93.102 netmask 255.255.255.0
Router-NAT(config)#ip nat pool ISP-B 202.102.100.100 202.102.100.102 netmask 255.255.255.0
```



提 示

地址池中的地址不能随便使用，必须通过互联网申请获得。

03 为内网用户配置 PAT 转换关系。

```
Router-NAT(config)#ip nat inside source list 100 pool ISP-A overload
Router-NAT(config)#ip nat inside source list 101 pool ISP-B overload
```



依照以上配置可以实现区分目标运营商网络，进行匹配的 NAT 转换。考虑到要实现基于端口的动态 NAT 转换，所以配置命令后的 overload 不能省略。

3）为外网访问内网 Web 服务器配置静态 NAT 转换

为了确保服务器访问的稳定性，一般对外发布的服务器都需要在网络出口做静态的NAT转换，具体配置命令如下。

```
Router-NAT(config)#ip nat inside source static tcp 192.168.1.100 80 61.192.93.100 80 extendable
Router-NAT(config)#ip nat inside source static tcp 192.168.1.100 80 202.102.100.100 80 extendable
```



由于本案例是将同一个内部局部地址转换到多个内部全局地址，所以参数 extendable 不可忽略。

4）在路由器的内部和外部接口上启用 NAT

启用 NAT 转换的配置命令如下。

```
Router-NAT(config)#int s0
Router-NAT(config-if)#ip nat outside
Router-NAT(config-if)#int s1
Router-NAT(config-if)#ip nat outside
Router-NAT(config-if)#int f0/1
Router-NAT(config-if)#ip nat inside
```



此处有两个外接口，都需要进行配置。

5）配置出口路由

为了确保内网可以访问外部网络，必须要在出口设备配置静态路由，具体配置命令如下。

```
Router-NAT(config)#ip route 61.192.93.0 255.255.255.0 s0
//到达 ISP-A 的流量指定从 S0 口路由转发
Router-NAT(config)#ip route 0.0.0.0 0.0.0.0 s1 //配置默认路由指定从 S1 口路由转发，确保到达 ISP-B 的流量从该口转发
Router-NAT(config)#ip route 0.0.0.0 0.0.0.0 s0 120    //浮动静态路由，可以称作备份路由
```



配置静态路由时可以指定转发到下一跳设备的 IP 地址，但是本地设备不一定会知道下一跳地址是多少，所以本实例指定本地设备接口编号进行路由转发。

至此为止，出口 NAT 的双线接入已经配置成功，在现实网络中地址配置可能会相对复杂，运

营商的地址段不可能是简单的一个小网段，需要管理员结合实际情况进行地址配置。

3.6 企业分支机构通信安全

传统的网络一般局限于一定的区域内，即便一个企业的多个分支机构需要跨越区域互连，也会采用帧中继、专线等广域网技术进行连接。但是传统方式费用高，架设复杂，很难满足日益增加的网络应用，需要有更便捷、更安全、更节约的方式进行跨区域分支连接。

传统的网络连接方式无法满足越来越多的 SOHO 一族的办公需求，需要有便捷、安全的连入企业内部网络的技术。VPN 虚拟专用网技术实现了这些网络应用需求，下面将详细介绍 VPN 技术的原理及其应用。

3.6.1 VPN 技术介绍

VPN 技术从产生至今，得到了飞速的发展和社会的认可，各行各业都在使用这项技术，它的出现使得帧中继和专线技术几乎被淘汰。下面详细了解一下 VPN 技术的原理及优势。

1. VPN 技术概述

VPN（Virtual Private Network），即虚拟专用网络。该技术用于实现局域网络之间通过 Internet 公共网络安全地传递数据。

互联网是目前最大的公共网络，其内有充足的资源可以利用。而 VPN 技术就是利用这一点，在 Internet 公共网络内部构建一条虚拟的连接广域网中不相邻的两个局域网的链路，该链路可以实现数据安全可靠的传输。VPN 技术的特征可以总结为以下几点。

（1）在混杂的公用网络（通常是 Internet 网络）中建立的一条临时的、安全的连接，是一条横穿公用网络的安全、稳定的隧道。

（2）具有强大的安全加密技术。

（3）可用于满足企业内部网络扩展的需求，允许与远程用户、分支机构和商业伙伴的内部网络建立安全可靠的连接。

（4）解决了不断增长的移动办公用户的互联网访问需求。

2. VPN 的优点

VPN 技术和传统的网络互连技术比较起来有很多优势，例如解决了长距离通信的费用成本，充分利用了互联网资源，可以实现快速、安全的网络扩展。下面以传统网络中使用比较多的专线技术和 VPN 技术作比较。

1）DDN 专线

使用 DDN 专线技术需要在两端局域网之间建立一条与互联网隔离的物理连接链路，如图 3-13 所示的网络拓扑图。

总的来说 DDN 专线技术存在以下不足：费用高、灵活性差、广域网的管理麻烦、拓扑结构复杂。

2）VPN 技术

VPN 技术连接时，只要确保两端都可以连接互联网即可实现，如图 3-14 所示的网络拓扑图。总的来说 VPN 技术存在以下优势：费用低、灵活性好、简单的网络管理、隧道的拓扑结构。

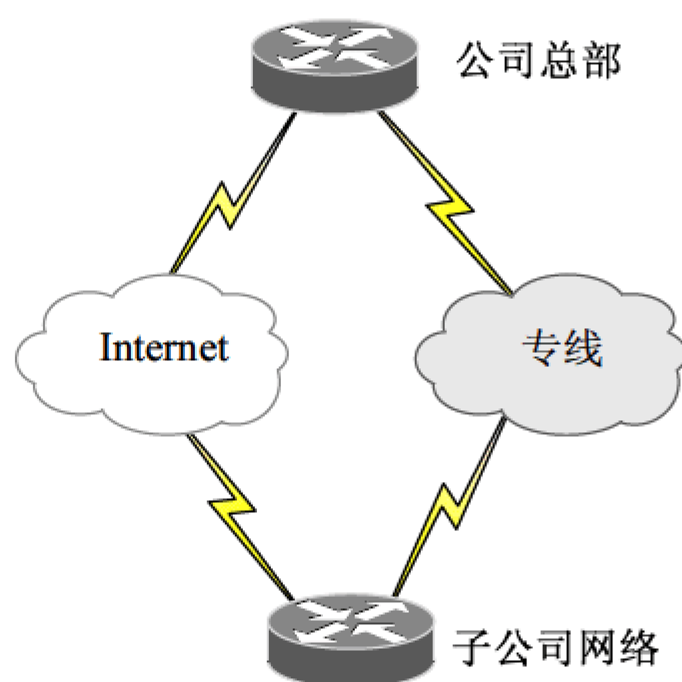


图 3-13　DDN 专线连网拓扑

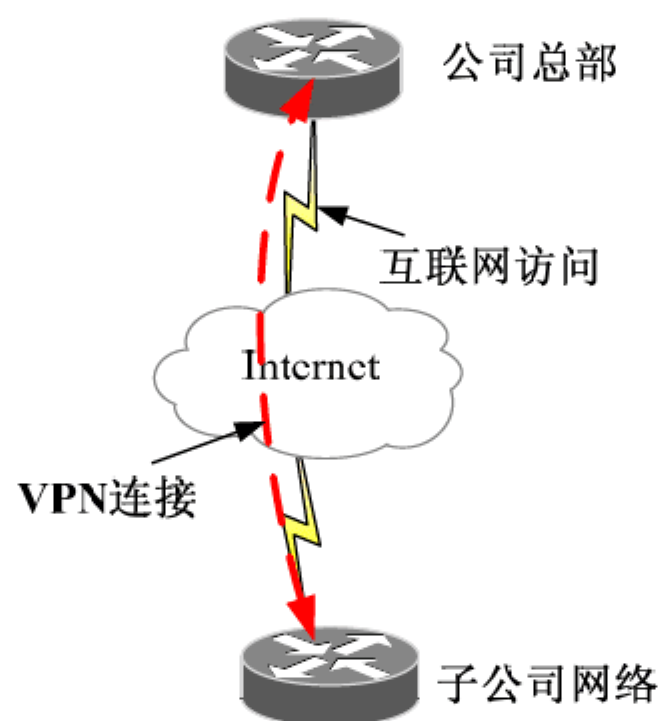


图 3-14　VPN 技术连网拓扑

使用 VPN 技术可以为用户带来很多好处，可以总结为以下几点。

（1）节省资金：VPN 技术免去了长途连接的费用，降低了 30%~70%的私有专网的建立费用。

（2）用户连接不受地点、网络接入方式的限制，只要用户愿意可以增加多条连接链路。

（3）提供安全性：具有强大的用户认证机制，可以有效地保障用户数据的安全性、完整性。

（4）配置便捷，不需要对现有网络结构和应用程序做调整。直接在现有环境基础上增加 VPN 配置即可，对于最终用户来说不会感觉到任何变化。

3. VPN 技术的工作原理

VPN 技术主要依靠认证加密和隧道技术来实现，图 3-15 所示是其工作原理图。

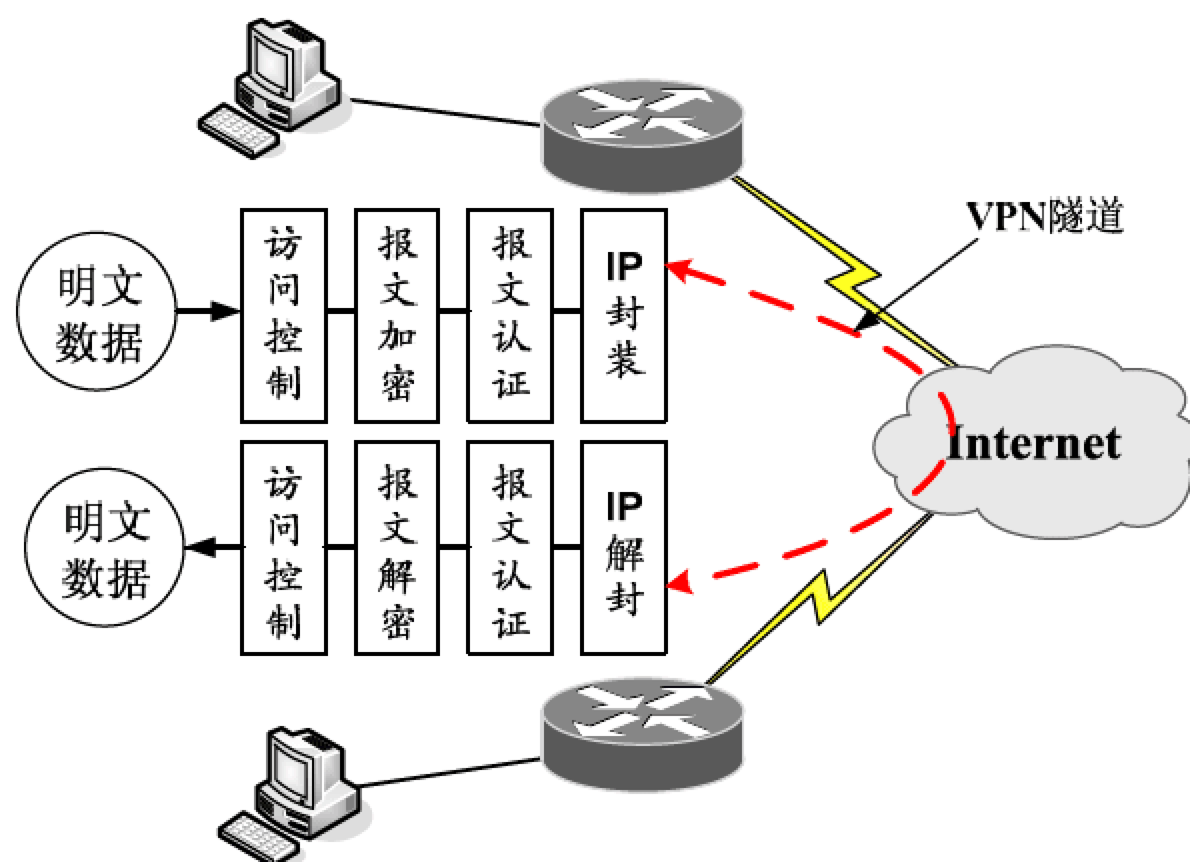


图 3-15　VPN 工作原理

实现 VPN 连接时使用了以下几种技术。

（1）安全隧道技术：隧道是在公共网络上传递私有数据的一种方式，而安全隧道是在公网上几个局域网之间进行数据传输中，保证数据安全和完整的技术。

（2）信息加密技术：用于实现数据传输过程中的安全，VPN 技术采用了多种加密技术，而且可以支持多种加密级别。

（3）用户认证技术：用于确保 VPN 的通信方的身份确认及合法。

（4）访问控制技术：用于限制 VPN 的通信双方的信息流。

VPN 技术在建立隧道时可以构建二层隧道和三层隧道。

（1）二层隧道 VPN 涉及以下协议。

① L2TP（Layer 2 Tunnel Protocol）：二层隧道协议，用于实现二层隧道的建立。

② PPTP（Point To Point Tunnel Protocol）：点到点隧道协议。

③ L2F（Layer 2 Forwarding）：用于实现二层隧道数据转发。

（2）三层隧道 VPN 涉及以下协议。

① GRE（General Routing Encapsulation）：用于实现三层隧道的建立。

② IPSec（IP Security Protocol）：IP 安全协议，用于实现三层隧道转发时数据的安全加密、认证。

4. VPN 技术分类

VPN 技术根据两端的连接主体不同，可以分为两种连接方式：远程访问的 VPN 和站点到站点的 VPN。

远程访问的 VPN 适用于建立临时性的 VPN 连接，家庭和移动办公用户使用得比较多。只需要企业网络中配置有软件或硬件形式的 VPN 设备，移动或家庭办公用户就可以通过自己的客户端操作系统直接建立 VPN 连接请求。

站点到站点的 VPN 连接可以建立长期的 VPN 连接，适合公司总部和子公司之间长期进行数据传输。需要两端网络中都有配置好的 VPN 软件程序或硬件设备，并且有匹配的认证加密配置。通常为了安全都会建立 IPSec VPN。

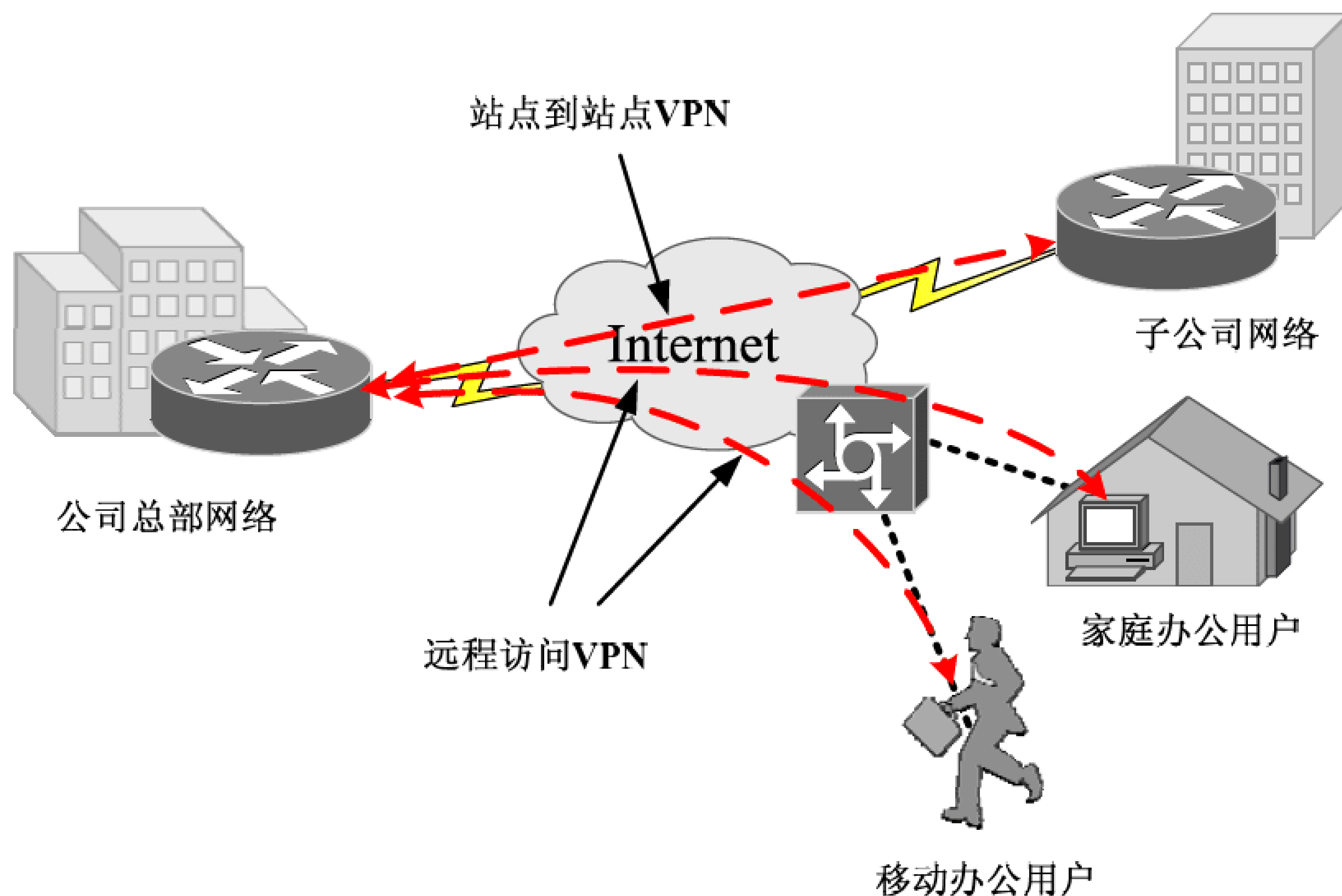


图 3-16　VPN 技术的分类

3.6.2　IPSec VPN 配置原理

IPSec（IP Security）是 IETF 为保证在 Internet 上传送数据的安全保密性而制定的框架协议。该协议应用在网络层，用于保证和认证用户 IP 数据包。IPSec 本身是开放的框架式协议，包含的各种算法之间是相互独立的，而且可以确保信息的机密性、数据的完整性、用户的验证和防重发保护。所以在假设 VPN 时通常会使用 IPSec 协议提供数据安全。

IPSec VPN 可使用的模式有两种：隧道模式和传输模式。使用隧道模式，IPSec 对整个 IP 数据包进行封装和加密，隐蔽了源和目的 IP 地址，从外部看不到数据包的路由过程，比较安全。使用传输模式，IPSec 只对 IP 有效数据载荷进行封装和加密，IP 源和目的 IP 地址不加密传送，安全程度比较低。

IPSec 主要由 AH、ESP 和 IKE 组成。AH (Authentication Header)是认证头协议，用于隧道中报文的数据源鉴别、数据的完整性保护，可以对每组 IP 包进行认证，防止黑客利用 IP 进行攻击。ESP(Encapsulation Security Payload)是封装安全载荷协议，用于保证数据的保密性，提供报文的认证性、完整性保护。IKE（Internet Key Exchange）是因特网密钥交换协议，在 IPSec 网络中用于密钥管理，为 IPSec 提供了自动协商交换密钥、建立安全联盟的服务。

在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由 SA（安全关联）进行定义。配置 SA 是配置其他 IPSec 的前提，它定义了通信双方保护数据流的策略。一般 SA 应当包含以下参数。

（1）使用的认证/加密算法、密钥长度等参数。

（2）指定认证和加密时需要的密钥字符串。

（3）确定需要使用该 SA 的数量流。

（4）IPSec 协议采用的封装协议和模式。

结合以上内容，可以通过以下几步完成 IPSec VPN 的配置。

01 为 IPSec VPN 开启 IKE 协议，并创建 IKE 协商。

```
Router(config)# crypto isakmp enable                //启动 IKE 协议功能
Router(config)# crypto isakmp policy priority       //创建 IKE 协商策略，priority 表示协商策略名
```

02 配置 IKE 的协商策略，即配置 SA（安全关联）的相关参数。

```
Router(config-isakmp)# authentication pre-share        //认证方法启用预共享密钥
Router(config-isakmp)# encryption ｛ des | 3des ｝      //设置加密算法
Router(config-isakmp)# hash ｛ md5 | sha1 ｝            //设置认证算法
Router(config-isakmp)# lifetime seconds                 //设置 SA 的活动时间
Router(config)# crypto isakmp key keystring address peer-address    //指定共享密钥和对端设备地址
Router(config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]
//设置传输模式集
Router(config)# access-list access-list-number {deny | permit} protocol source source-wildcard destination
destination-wildcard        //为受保护数据流配置访问控制列表
```

03 创建加密图，并将其应用到端口，加密图用于关联 IKE 协商策略和受保护数据流。

```
Router(config)# crypto map map-name seq-num ipsec-isakmp      //创建加密图
Router(config-crypto-map)# match address access-list-number   //关联受保护数据流
```

```
Router(config-crypto-map)# set peer ip_address                //指定对端设备地址
Router(config-crypto-map)# set transform-set name             //指定启用的传输模式名称
Router(config)# interface interface_name interface_num
Router(config-if)# crypto map map-name          //应用配置的加密图，并启用 IPSec VPN
```

04 配置完成后，可以通过以下命令进行调试或排错。

```
Router# show crypto isakmp policy                    //查看 IKE 策略配置
Router# show crypto ipsec transform-set              //查看 IPSec 传输方式配置策略
Router# show crypto ipsec sa                         //查看 SA 的配置参数
Router# show crypto map                              //查看加密图配置
```

提 示

配置 IPSec VPN 时隧道两端的设备配置参数必须对应匹配，否则 VPN 配置失败。

3.6.3 项目实战 8：使用 IPSec VPN 技术实现企业分支机构安全连接

企业分支机构或者商业伙伴之间如果需要进行频繁大量数据传输，就需要建立 VPN 连接。下面介绍一个企业 IPSec VPN 配置的案例。

1. 实验网络拓扑图

按照图 3-17 所示的网络拓扑图连接设备进行实验。

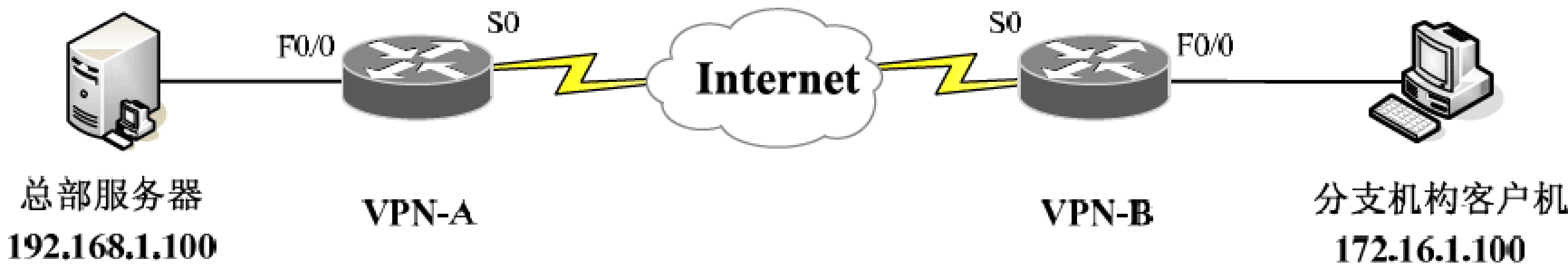


图 3-17 企业分支机构 VPN 连接拓扑图

依照图 3-17 为网络规划地址配置，地址分配如表 3-7 所示。

表 3-7 地址分配

设备	地址	设备	地址
VPN-A	F0/0:192.168.1.1/24 S0:202.102.100.1/24	VPN-B	F0/0:172.16.1.1/24 S0:202.102.100.2/24
总部服务器	192.168.1.100/24	分支机构客户端	172.16.1.100/24

2. 实验配置

企业分支机构使用 IPSec VPN 技术互连的操作方法如下。

1）设备基础配置

路由器和服务器设备的基本配置主要包括：设备命名、IP 地址配置、设备加密等常规配置，这些内容在前面小节中有介绍，这里不再演示。

2）配置出口设备 NAT 转换

VPN 是建立在两个局域网出口之间的隧道连接，所以两个 VPN 设备必须要能够满足内网访问互联网的要求，以及需要配置 NAT 技术。配置出口设备 NAT 转换的具体操作方法如下。

VPN-A：

01 定义需要被 NAT 的数据流。

```
VPN-A(config)#access-l 101 deny ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255
VPN-A(config)#access-l 101 permit ip 192.168.1.0 0.0.0.255 any
```


提 示

配置允许 NAT 转换的数据流时，一定要将建立 VPN 的流量排除在外，否则 VPN 将不可用。

02 定义 NAT 转换关系，这里使用的不是外部公共地址，而是连接互联网的接口。

```
VPN-A(config)#ip nat inside source list 101 interface s0 overload
```

03 在路由器上定义 NAT 的内部接口和外部接口。

```
VPN-A(config)#int f0/0
VPN-A(config-if)#ip nat inside
VPN-A(config)#int s0
VPN-A(config-if)#ip nat outside
```

VPN-B:

01 定义需要被 NAT 的数据流（即除去通过 VPN 传输的数据流）。

```
VPN-B(config)#access-l 101 deny ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255
VPN-B(config)#access-l 101 permit ip 172.16.1.0 0.0.0.255 any
```

02 定义 NAT 转换关系。

```
VPN-B(config)#ip nat inside source list 101 interface s0 overload
```

03 在路由器上定义 NAT 的内部接口和外部接口。

```
VPN-B(config)#int f0/0
VPN-B(config-if)#ip nat inside
VPN-B(config)#int s0
VPN-B(config-if)#ip nat outside
```

3）配置 IPSec VPN

为分支机构配置 VPN 连接，具体配置步骤如下。

VPN-A：

01 定义感兴趣的数据流，即将来需要通过 VPN 加密传输的数据流。

```
VPN-A(config)#access-list 102 permit ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

02 定义 ISAKMP 策略。

```
VPN-A(config)#crypto isakmp enable          //启用 ISAKMP(IKE)
```

```
VPN-A(config)#crypto isakmp policy 10
VPN-A(config-isakmp)#authentication pre-share //认证方法使用预共享密钥
VPN-A(config-isakmp)#encryption des       //加密方法使用 des
VPN-A(config-isakmp)#hash md5             //散列算法使用 md5
VPN-A(config-isakmp)#group 2              //DH 模长度为 1024
```

03 将 ISAKMP 预共享密钥和对等体关联，预共享密钥为“cisco”。

```
VPN-A(config)#crypto isakmp identity address
VPN-A(config)#crypto isakmp key cisco address 202.102.100.2
```

04 设置 IPSec 转换集。

```
VPN-A(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
VPN-A(cfg-crypto-trans)#mode tunnel
```

05 设置加密图。

```
VPN-A(config)#crypto map cisco 10 ipsec-isakmp
VPN-A(config-crypto-map)#match address 102   //加载感兴趣流
VPN-A(config-crypto-map)#set peer 202.102.100.2   //设置对等体地址
VPN-A(config-crypto-map)#set transform-set ccie   //选择转换集
VPN-A(config-crypto-map)#set pfs group2 //设置完美前向保密，DH 模长度为 1024
```

06 在外部接口上应用加密图。

```
VPN-A(config)#int s0
VPN-A(config-if)#crypto map Cisco
```

VPN-B:

01 定义感兴趣的数据流，即将来需要通过 VPN 加密传输的数据流。

```
VPN-B(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255
```

02 定义 ISAKMP 策略。

```
VPN-B(config)#crypto isakmp enable        //启用 ISAKMP(IKE)
VPN-B(config)#crypto isakmp policy 10
VPN-B(config-isakmp)#authentication pre-share //认证方法使用预共享密钥
VPN-B(config-isakmp)#encryption des       //加密方法使用 des
VPN-B(config-isakmp)#hash md5             //散列算法使用 md5
VPN-B(config-isakmp)#group 2              //DH 模长度为 1024
```

03 将 ISAKMP 预共享密钥和对等体关联，预共享密钥为“Cisco”。

```
VPN-B(config)#crypto isakmp identity address
VPN-B(config)#crypto isakmp key cisco address 202.102.100.1
```

04 设置 IPSec 转换集。

```
VPN-B(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
VPN-B(cfg-crypto-trans)#mode tunnel
```

05 设置加密图。

```
VPN-B(config)#crypto map cisco 10 ipsec-isakmp
```

```
VPN-B(config-crypto-map)#match address 102   //加载感兴趣流
VPN-B(config-crypto-map)#set peer 202.102.100.1   //设置对等体地址
VPN-B(config-crypto-map)#set transform-set ccie   //选择转换集
VPN-B(config-crypto-map)#set pfs group2 //设置完美前向保密，DH 模长度为 1024
```

06 在外部接口上应用加密图。

```
VPN-B(config)#int s0
VPN-B(config-if)#crypto map Cisco
```

3.7 专家答疑

（1）很多底层的傻瓜式交换机无法配置 VLAN，核心交换机配置的 VLAN 底层设备能识别吗？

答：如果将一个区域的网络分配到了除 VLAN1 外的其他 VLAN，那么这个区域的底层交换机必须要能够支持识别这个 VLAN，然而一般傻瓜式交换机是无法配置 VLAN 的，这确实很让人困惑。为了解决这一问题，很多厂商的傻瓜式交换机配置了可默认识别上层 VLAN 的功能，以及自适应上层设备的 VLAN 配置，但是并不一定可以设置所有的 VLAN，有可能只能识别有限数量的 VLAN，这可以查看不同设备的说明书。

从目前的技术来说，底层设备 VLAN 配置的问题是不会影响整个网络 VLAN 配置策略的实施的。

（2）在实现企业分支机构互连时，是否需要购置专业的 VPN 设备？

答：目前实现分支机构之间安全互连的最好方法就是使用 VPN 技术，VPN 以其安全、便捷而著称，因此市场上出现了很多 VPN 专用设备。这些所谓的 VPN 设备是否真的有必要购买呢？这还要看情况分析，目前市场上大多数的出口设备，如代理服务器、防火墙、出口路由器等都有 VPN 配置功能，但是很多企业出口的设备比较简陋，虽然有 VPN 配置功能，而设备本身的安全性却并不高，这很可能会造成不必要的网络攻击。

所以如果企业出口设备整体的性能、稳定性、安全性都比较好的情况下可以不适用专业的 VPN 设备，如果出口设备比较简陋，是建议购置专业的 VPN 设备的。

第 4 章　企业无线网络管理与维护

随着网络的发展，人们对网络的要求越来越高，需要随时随地地访问互联网，这时无线网络就应运而生。无线网络是利用电磁波来作为数据传输的媒介，就应用层面而言，与有线网络的用途完全相似，最大的不同是传输信息的媒介不同。

4.1　无线局域网概述

WLAN 利用电磁波在空气中发送和接收数据，而无需线缆介质。它是对有线连网方式的一种补充和扩展，使网上的计算机具有可移动性，能快速方便地解决使用有线方式不易实现的网络连通问题。

随着笔记本、具有 WiFi 功能的手机、PDA（个人数字助理）等无线客户端的流行，无线网络越来越受到人们的青睐，无线网络的特征是以一个固定的信息点为基础，形成一个网络覆盖面，对于无线终端用户来说，只要无线网卡能搜索到无线信号，就可以随时随地地访问互联网，无线网络带来的便捷性不言而喻。与有线网络相比，WLAN 具有的优点有以下几方面。

1. 免去布线的麻烦

传统的计算机使用网线连接至互联网，但是很多时候受到房间各种原因的限制，线缆不能连接，例如在外租房，大部分房东不愿意在屋内凿洞拉线，这时候上网就成了问题。如果采用无线网络，只需要在 ISP 运营商接口连接一根线缆至屋内无线路由器上，无线客户端不需要线缆可以直接连接至互联网。

2. 减少投资

无线网络没了线缆的连接，就减少了线缆和施工的费用，只要购买性能良好的无线 AP 即可，可以节约很大的成本。

3. 随时随地上网

现在无线校园、无线城市的兴起，使得人们可以在无线校园内部、无线城市内部随时随地上网，不需要受到没有网线的限制。

4. 安装便捷

一般的网络建设中，施工时间较长，并且会对周围的环境造成一定的影响。而无线网络的优

势在于大量减少了网络布线的工作量，只需要在合适的位置安装相应的无线 AP 设备，就可以建立满足需求的无线网络。

4.2　无线网络方案实施

随着因特网的广泛应用，人们对于移动接入互联网的需求不断增加。无线网络作为有线网络的有效补充，凭借着投资小、建设周期短、方便灵活等特点，正在逐步成为人们接入互联网的常用选择。

4.2.1　无线网络需求分析

现在全国许多住宅小区和学校都还没有无线网络覆盖，并且大部分的小区建设较早，不适合进行网络布线，此时无线网络的优点就更显现出来。

（1）无线网络既然是“无线”，所以就没有铺设或者改造物理线路的问题，就不会破坏已有的设施，组建无线网络更加方便。

（2）无线网络组建简单，只需要根据无线网络设计，在合适的位置安装无线 AP，然后在客户端安装无线接入端，而不需要在室内室外穿墙打洞，甚至是入户施工，这样会得到居民的配合，缩短施工周期。

（3）无线网络因为运行原理的问题，无线网络的投入较有线网络的投入更低。对于无线用户，如果每户的投入成本为 2000 元，100 个用户则需要 20 万元，如果采用有线的方式，一个小区为 1000 户，每个信息点需要 800 元，无论开通率为多少，必须一次投入 80 万元。目前小区宽带接入率普遍不高（一般在 5%左右，最高的也只能达到 20%）。

（4）扩展灵活，避免浪费。无线的灵活性可以让 ISP 随着用户数目的增加来增加 AP 的数目。而有线的方式则不管用户有多少，信息点都必须提前布好，这样就造成了大量的浪费。

（5）用户数据安全性的需求。无线网络产品可以通过加密、MAC 控制来保证系统的安全性。无线系统可以将每个用户进行隔离，保证不会被“网络邻居”访问，造成共享文件丢失或受到破坏。

4.2.2　无线网络方案设计

目前，无线网络的接入方式主要有两种：对等无线网络和独立无线网络。

1. 对等无线网络

计算机与计算机之间通过无线网卡进行连接，构建成简单的无线网络，如图 4-1 所示。在这样的无线网络中，计算机与计算机之间的地位是相等的，被称为对等无线网络。网络中的计算机之间没有物理线缆的连接，但是因为无线网卡的连接，计算机之间可以实现网络和资源的共享。

因为无线网络的传输距离有限，因此在对等无线网络中，计算机与计算机之间的距离必须在无线网卡的信号覆盖范围之内，否则将不能进行通信。一般情况下无线网卡的信号的有效传输距离（也就是无线网络的最大直径）为 30m 左右。另外在对等无线网络中，计算机与计算机之间共享

连接带宽，并且无线网络的带宽有限，因此对等网络只适用于计算机数量较小并且对传输速率没有较高要求的小型网络。所以，无线网络一般用在家庭网络或者小型的办公网络中。

2. 构架无线网络

计算机与计算机之间的无线网卡通过一个中央节点连接，信号的发送和接收通过该中央节点进行，这样的无线网络被称为构架无线网络。如图 4-2 所示，中央节点称为无线 AP，无线 AP 具有发射和接收无线信号的功能。

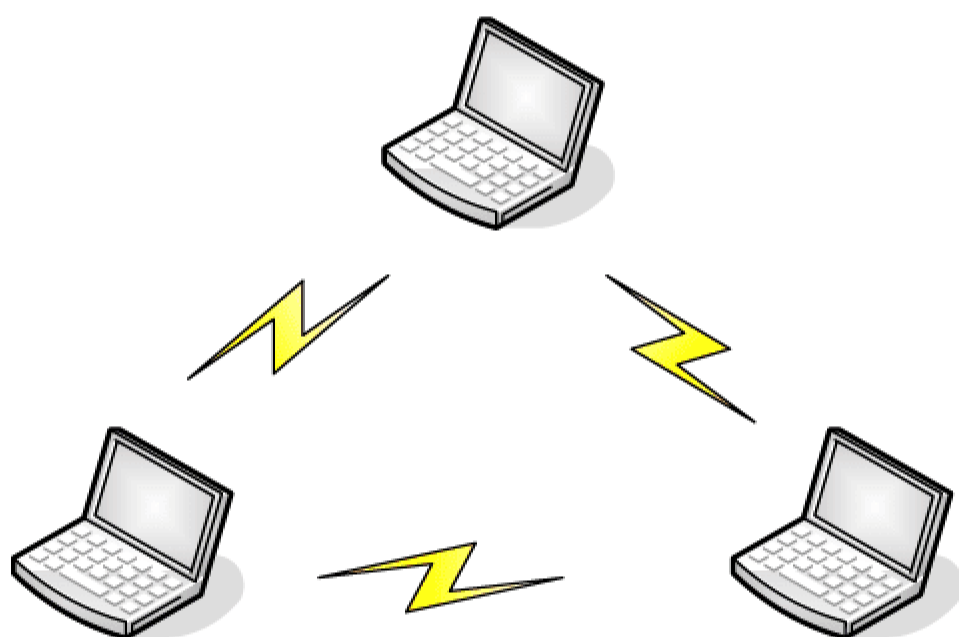


图 4-1　对等无线网络

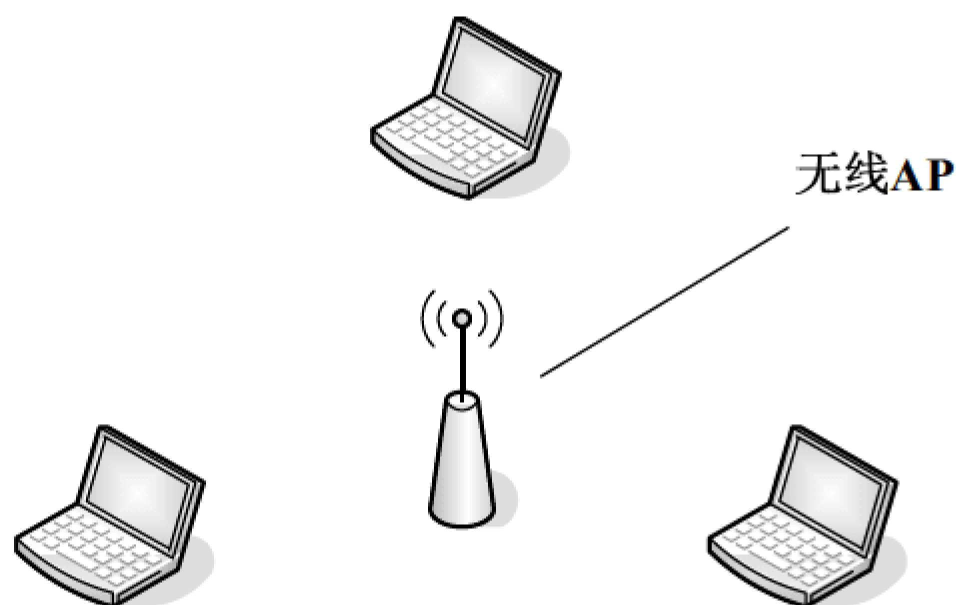


图 4-2　构架无线网络

和对等无线网络相比，构架无线网络中加入了无线 AP，无线 AP 类似于有线网络中的集线器或者是交换机，无线网络中计算机之间的通信完全依赖于无线 AP，因此无线 AP 的功率就决定了无线网络的覆盖范围，其覆盖范围较大。

需要注意的是，该方案仍然属于共享式接入，也就是说，虽然传输距离比对等无线网络增加了一倍，但所有计算机之间的通信仍然共享无线网络带宽。由于带宽有限，因此该无线网络方案仍然只能适用于小型网络。

4.2.3　规划无线 AP 的分布

目前主流的无线协议都是由 IEEE（美国电气电工协会）所制定，IEEE 认定的四种无线标准分别为 IEEE802.11b、IEEE802.11g、IEEE802.11a 和 IEEE802.11n。

IEEE802.11b 采用 2.4GHz 频带，调制方法采用补偿码键控（CKK），传输速率能够从 11Mbps 自动降到 5.5Mbps，或者根据直接序列扩频技术调整到 2Mbps 和 1Mbps，以保证设备正常运行与稳定。IEEE802.11a 扩充了标准的物理层，规定该层使用 5GHz 的频带。该标准采用 OFDM 调制技术，传输速率范围为 6~54Mbps。不过此标准与 IEEE802.11b 标准并不兼容。支持该协议的无线 AP 和无线网卡，在市场上较少见。IEEE802.11g 同样运行于 2.4GHz，但向下兼容 IEEE802.11b，而由于使用了与 IEEE802.11a 标准相同的调制方式 OFDM（正交频分），因而能使无线局域网达到 54Mbps 的数据传输速率。IEEE802.11n 采用 2.4GHz 频带，调制方法采用补偿码键控（CKK），传输速率能够从 300Mbps 自动降到 5.5Mbps，或者根据直接序列扩频技术调整到 2Mbps 和 1Mbps，以保证设备正常运行与稳定。

综上所述，现在无线网络经常使用的协议为 IEEE802.11b/g/n，工作频率为 2.4～2.4835GHz。其中为了防止无线信号之间信号干扰，IEEE 将无线频段划分为 13 个信道，但是需要注意的是，13

个信道之间并不独立，信号之间依然会相互干扰。

当多个 AP 信号覆盖区域相互交叉重叠时，各个 AP 覆盖区域所占信道之间必须遵守一定的规范，邻近的相同信道之间不能相互覆盖，也就是说，相互覆盖区域的无线 AP 不能采用同一信道。否则，会造成 AP 在信号传输时的相互干扰，从而降低 AP 的工作效率。在可用的 13 个信道中，仅有 3 个信道是完全不覆盖的，它们分别是信道 1、信道 6 和信道 11，利用这些信道组建具有多个无线 AP 的无线网络是最合适的。另外，用于实现无线漫游网络的无线 AP 必须使用同一网络名称（SSID），使用同一网段的 IP 地址，否则无线客户端将无法实现漫游功能。

4.2.4　项目实战 1：配置无线路由器，并实现无线网络环境的安全加密

下面详细介绍如何建立无线网络，需要准备的硬件是无线路由器，本实例以 TP-LINK TL-WR340G+ 54M 型号无线路由器进行讲解，然后进行线缆的连接，图 4-3 所示为无线路由器的连接拓扑图。

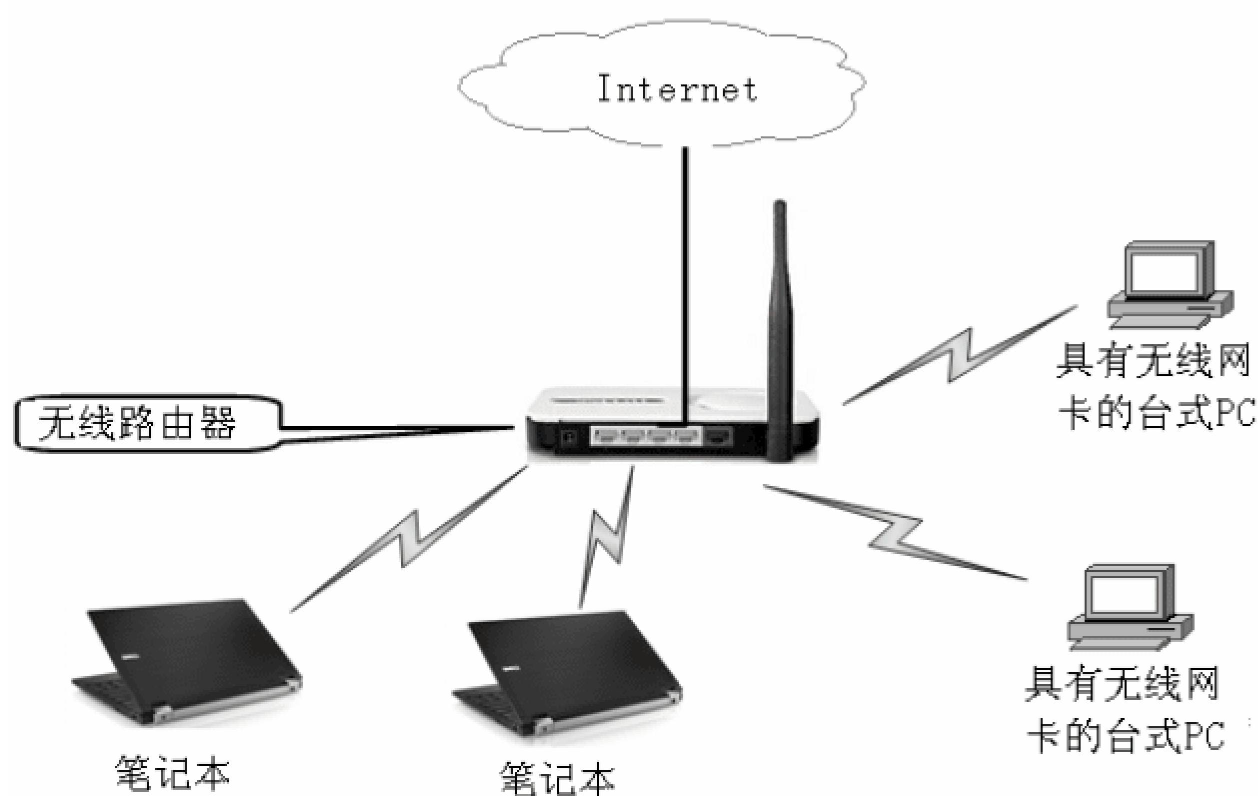


图 4-3　无线网络拓扑图

1. 开启路由器无线功能

建立家庭无线局域网的第一步是开启路由器无线功能，具体的操作步骤如下。

01 本机的 IP 地址设置为 192.168.1.0/24 网段，然后在 IE 浏览器的地址栏中输入 http://192.168.1.1，如图 4-4 所示，单击【转到】按钮。

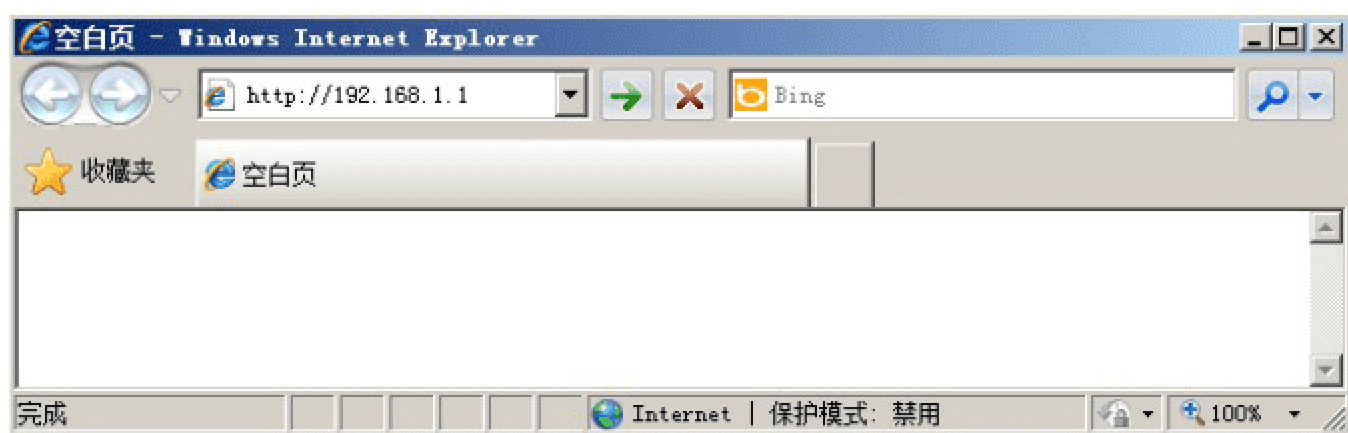


图 4-4　访问路由器


提　示

IP 地址设置哪个网段以及用什么 IP 地址访问路由器，具体需要参考《无线路由器使用操作说明书》，不过大部分的 TP-LINK 路由器默认 IP 地址都为 192.168.1.1。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，如图 4-5 所示，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，单击【确定】按钮。

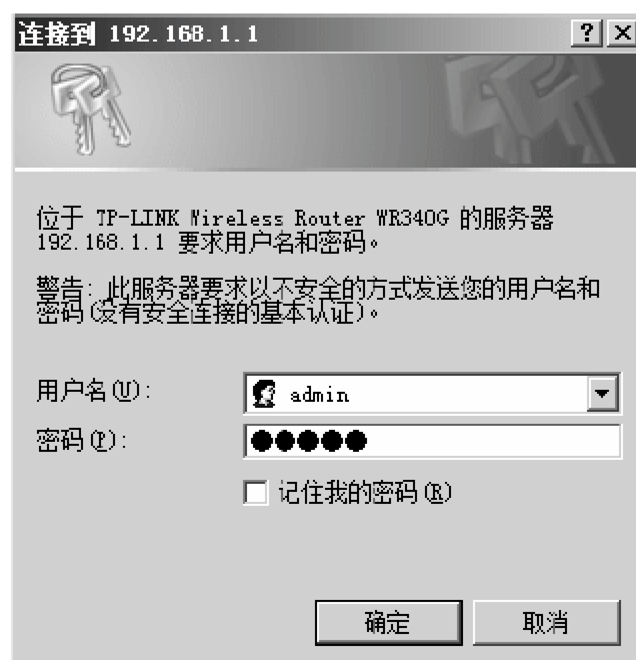


图 4-5 【连接到 192.168.1.1】对话框

03 弹出【TP-LINK】路由器的设置页面，如图 4-6 所示，选择左侧【网络参数】➢【WAN 口设置】选项，设置 TP-LINK 的上网方式。在【WAN 口连接类型】下拉列表中选择上网方式。一般情况下家庭都是通过 ADSL 方式（也就是电话线）上网，需要在【WAN 口连接类型】下拉列表中选择【PPPoE】选项，在【上网账号】和【上网口令】文本框中分别输入合法的上网账号和密码，单击【连接】按钮即可。



图 4-6 【TP-LINK】路由器的设置页面

04 选择左侧【网络参数】➢【LAN 口设置】选项，如图 4-7 所示，在【IP 地址】和【子网掩码】文本框中分别输入局域网内部计算机的网关和子网掩码，需要注意这个 IP 地址就是内部局域网计算机的网关，同时也是客户机访问 TP-LINK 路由器的 IP 地址，本实例中输入“192.168.1.1”，单击【保存】按钮即可。



图 4-7 【LAN 口设置】对话框

05 选择左侧【无线参数】➢【基本设置】选项，如图 4-8 所示，选择【开启无线功能】复选框，单击【保存】按钮，到此一个简单的无线路由器就设置完毕。

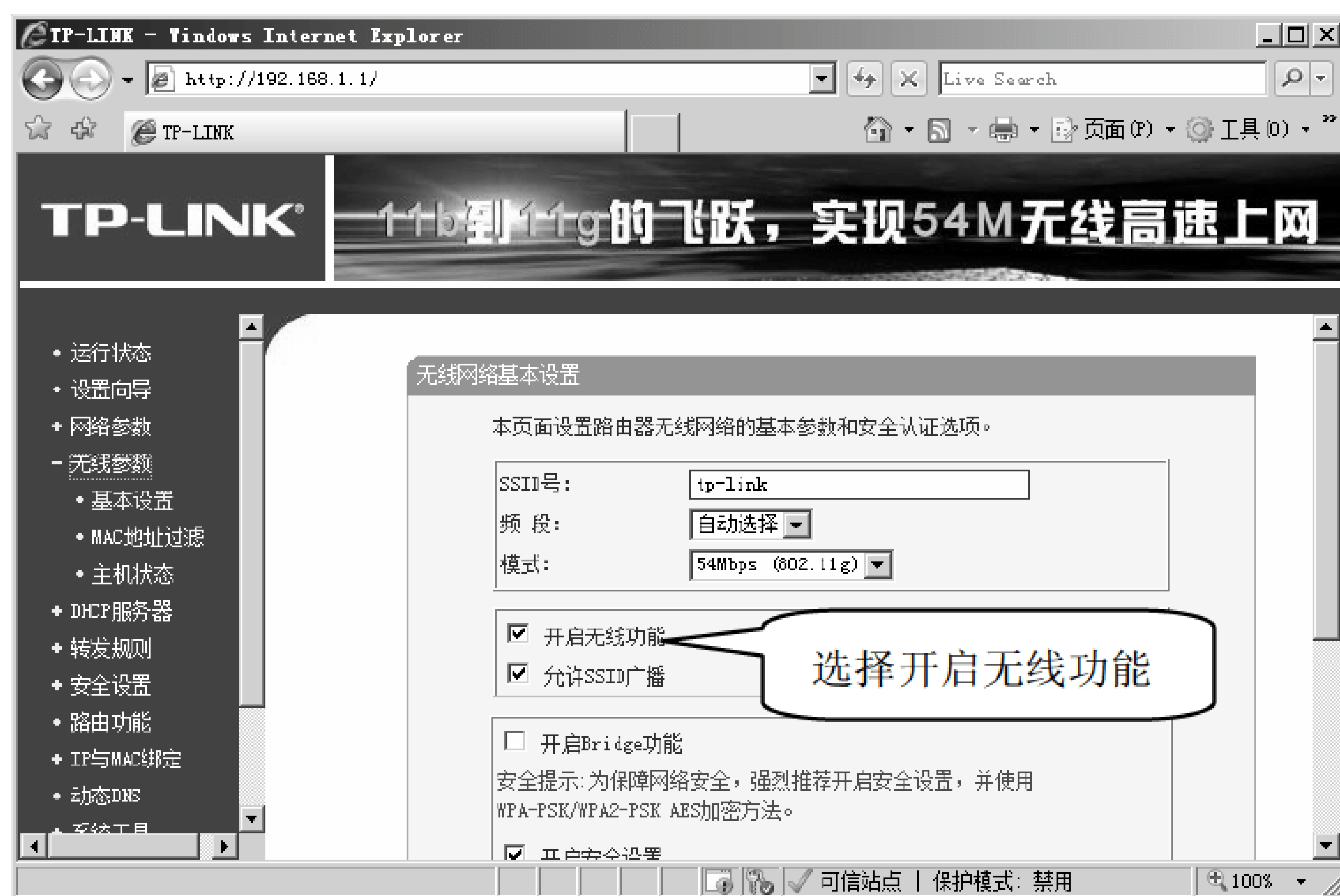


图 4-8 【无线参数】对话框

06 建立无线局域网的第二步是连接无线客户端，如图 4-9 所示，具体操作步骤如下。客户端连接无线路由器。本实例采用 Win7 系统的笔记本来作为无线客户端。单击系统桌面右下角的图标，会看到无线客户端自动扫描到区域内的所有无线信号。

07 右击扫描出现的 tp-link 信号，如图 4-10 所示，在弹出的快捷菜单中选择【连接】选项。



图 4-9　无线扫描信号



图 4-10　tp-link 信号

08 连接成功后，在系统右下角出现图标，将鼠标放在 tp-link 信号上面，可以看到该无线信号信息。如图 4-11 所示，此时该计算机就可以正常地访问互联网了。



图 4-11　客户端连接

2. 无线安全加密

无线网络不需要物理线缆，非常方便，但正因为无线网络是靠无线信号进行信息传输，而无线信号又不方便管理，因此，数据的安全性更是遭到了前所未有的挑战，于是各种各样的无线加密算法应运而生。

1）WEP 加密

相对于有线网络来说，通过无线局域网发送和接收数据更容易被窃听。设计一个完善的无线局域网系统，加密和认证是需要考虑的两个必不可少的安全因素。无线局域网中应用加密和认证技术的最根本目的就是使无线业务能够达到与有线业务同样的安全等级。针对这个目标，IEEE802.11

标准中采用了 WEP（Wired Equivalent Privacy，有线对等保密）协议来设置专门的安全机制，进行业务流的加密和节点的认证。它主要用于无线局域网中链路层信息数据的保密。

WEP 采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。WEP 使用加密密钥(也称为 WEP 密钥)加密 802.11 网络上交换的每个数据包的数据部分。启用加密后，两个 802.11 设备要进行通信，必须具有相同的加密密钥，并且均配置为使用加密。如果配置一个设备使用加密而另一个设备没有，则即使两个设备具有相同的加密密钥也无法通信。也就是说所有无线客户端和无线接入点必须使用一个共享的加密密钥进行加密，密钥越长，黑客破解的时间越长，也就越安全。

下面详细介绍无线网络 WEP 加密的具体方法。

（1）设置无线路由器 WEP 加密数据。

设置无线路由器 WEP 加密数据具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，访问无线路由器，单击【转到】按钮。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 家用路由器的默认用户名和密码都为“admin”，单击【确定】按钮。

03 单击左侧【无线参数】➢【基本设置】选项，如图 4-12 所示，选中【开启安全设置】复选框，在【安全类型】下列表单中选择【WEP】选项，在【密钥格式选择】下拉列表中选择【ASCⅡ码】选项。设置密钥，在【密钥 1】后面的【密钥类型】下拉列表中选择【64 位】选项，在【密钥内容】文本框中输入要使用的密码，本实例输入密码为“cisco”，单击【保存】按钮。

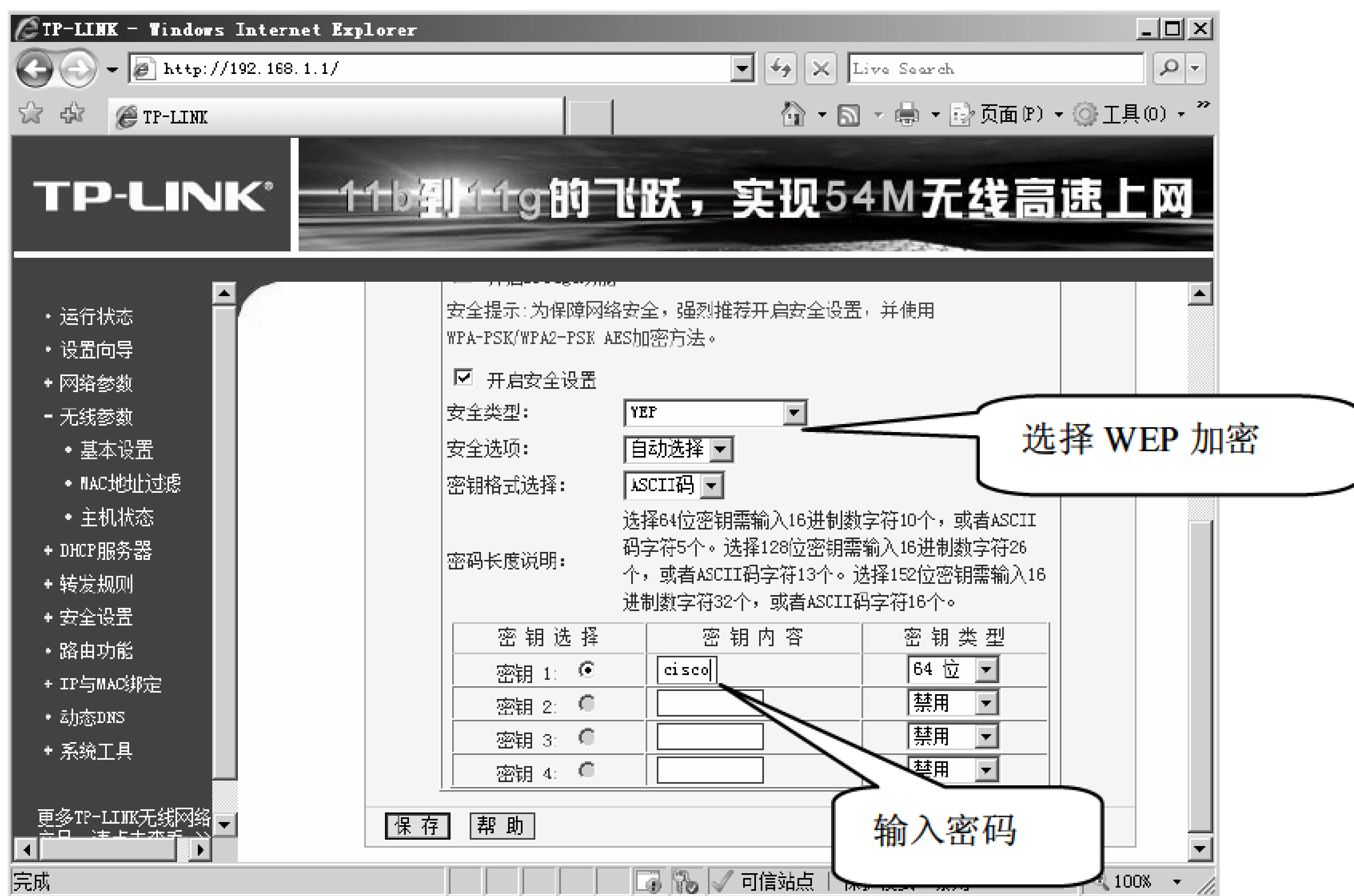


图 4-12　【无线参数】对话框

（2）客户端连接。

需要 WEP 加密认证的无线客户端连接的具体操作步骤。

01 单击系统桌面右下角图标，如图 4-13 所示，无线客户端自动扫描到区域内的所有无线信号。

02 右击 tp-link 信号，如图 4-14 所示，在弹出的快捷菜单中选择【连接】选项。



图 4-13 扫描无线信号



图 4-14 tp-link 信号

03 弹出【连接到网络】对话框，如图 4-15 所示，在【安全密钥】文本框中输入密码“cisco”，单击【确定】按钮。

04 单击系统桌面右下角图标，如图 4-16 所示，将鼠标放在 tp-link 信号上，可以看到无线信号的连接情况，图 4-16 所示表明已经成功连接无线路由器。



图 4-15 【连接到网络】对话框



图 4-16 tp-link 信号

2）WPA 加密

早期的 WEP 无线加密算法在无线网络的数据安全方向起到了很大的作用，但是 WEP 使用的是静态的密钥而非动态密钥，导致 WEP 密码很容易被监听到或者破解，因此在组建无线网络的时候，理想的做法是用 WPA 和 WPA2 加密算法来代替 WPA。

WPA 算法主要用于增强无线局域网系统的数据保护和访问控制水平，采用了动态的加密密钥。WPA2 是在 WPA 的基础之上，经由 WiFi 联盟验证过的 IEEE802.11i 标准的验证形式，是目前公认

的比较安全的无线加密算法。

WPA 作为 WEP 的升级版，在安全性上有了很大的改进，主要体现在身份验证、加密机制和数据包检查等方面，并且 WPA 使用了动态的密钥，使得黑客破解起来相当费力。但是完整的 WPA 设置比较复杂，一般用户很难操作，导致 WPA 和 WPA2 算法在实际中应用很少，除非对无线网络要求苛刻的公司。

3）WPA-PSK 安全加密算法

由于 WPA 操作复杂，因此不管是在家庭还是在公司的应用中经常采用 WPA 的简化版：WPA-PSK 和 WPA2-PSK。WPA-PSK 可以看成是一个认证机制，只要求一个单一的密码进入每个无线局域网节点（例如无线路由器），只要密码正确，就可以使用无线网络。

WPA-PSK 安全加密机制和 WPA 是相同的，两者的区别是：WPA-PSK 认证被简化为只要一个简单的密码，而不需要设置复杂的身份证明等信息。WPA-PSK 的缺点是：同 WEP 一样也会受到黑客的破解。但是因为密钥是动态的，其安全性比 WEP 要强很多。

下面介绍如何使用 WPA-PSK 或者 WPA2-PSK 加密无线网络。

（1）设置无线路由器 WPA-PSK 安全加密数据。

设置无线路由器 WPA-PSK 安全加密的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，单击【转到】按钮。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，单击【确定】按钮。

03 选择左侧【无线参数】➢【基本设置】选项，如图 4-17 所示，选中【开启安全设置】复选框，在【安全类型】下拉列表中选择【WPA-PSK/WPA2-PSK】选项，在【安全选项】和【加密方法】下拉列表中分别选择【自动选择】选项，在【PSK 密码】文本框中输入加密密码，本实例设置密码为“sushi1986”，单击【保存】按钮。

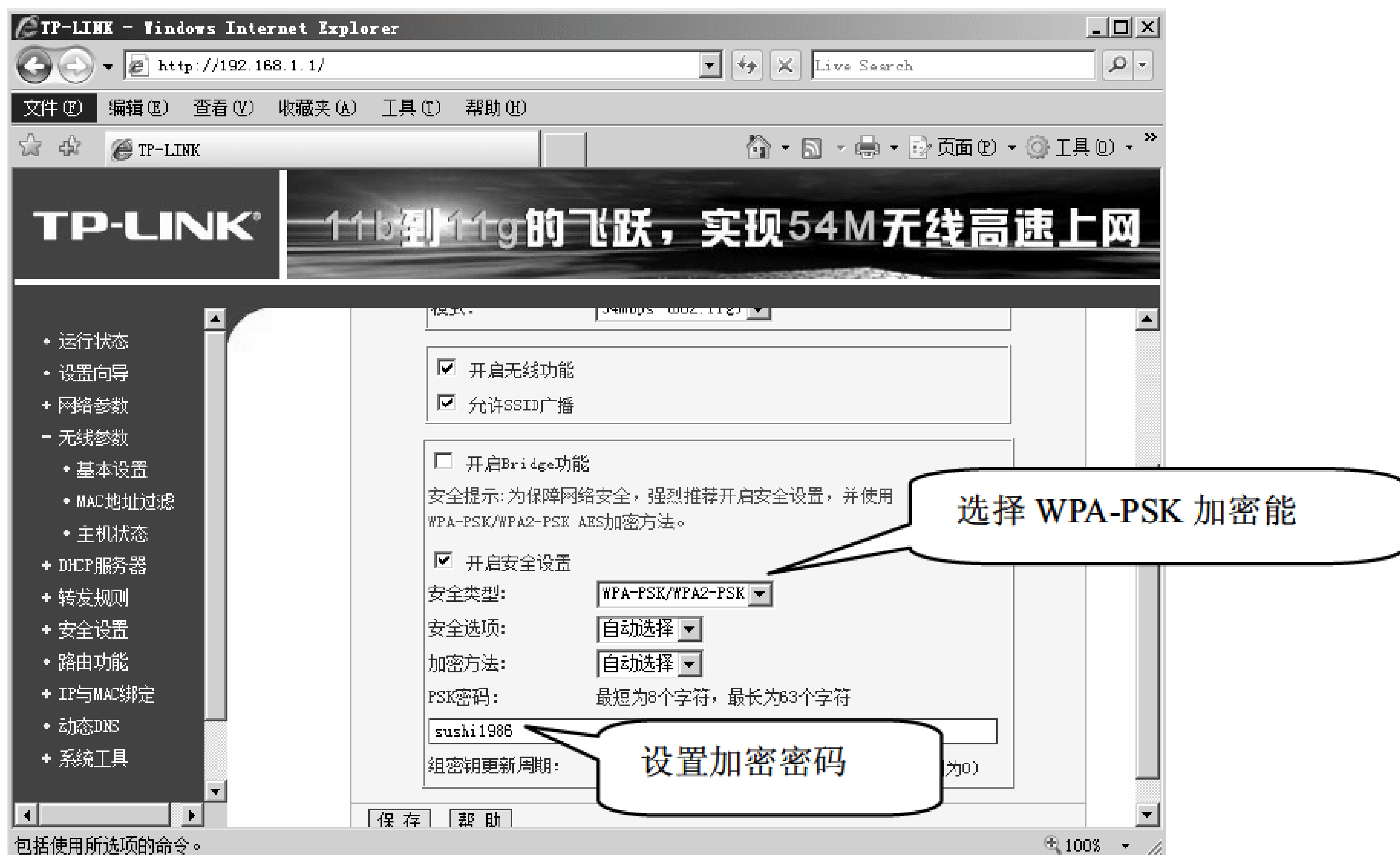


图 4-17　【无线参数】对话框

04 弹出【Windows Internet Explorer】提示对话框，如图 4-18 所示，单击【确定】按钮，重新启动路由器即可。

（2）客户端连接。

使用 WPA-PSK 安全加密认证的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角图标，如图 4-19 所示，无线客户端会自动扫描区域内的无线信号。

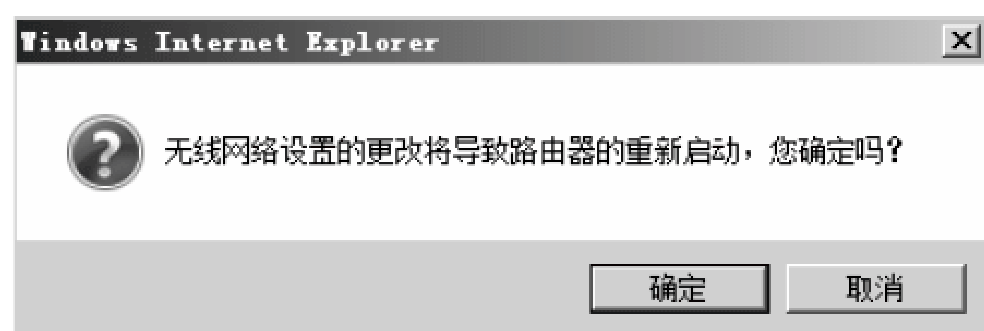


图 4-18 【Windows Internet Explorer】提示对话框



图 4-19 扫描无线信号

02 右击 tp-link 信号，如图 4-20 所示，在弹出的快捷菜单中选择【连接】命令。

03 弹出【连接到网络】对话框，如图 4-21 所示，在【安全密钥】文本框中输入密码“sushi1986”，单击【确定】按钮。



图 4-20 tp-link 信号



图 4-21 【连接到网络】对话框

04 单击系统桌面右下角图标，如图 4-22 所示，将鼠标放在 tp-link 信号上，可以看到无线

信号的连接情况，图 4-22 所示表明已经成功连接无线路由器。



图 4-22　tp-link 信号



提　示

在 WPA-PSK 加密算法的使用过程中，密码设置应该尽可能复杂，并且要注意定期更改密码。

3. 设置独特的 SSID

SSID（Service Set Identifier）主要用来区分不同的无线网络，相当于给每个无线网络设置了 ID 号码，只有当无线客户端和无线 AP 的 SSID 一样时，才可以进行通信。一般情况下，无线网络的 SSID 在无线 AP 上进行设置并有 AP 广播出来，经过无线客户端的扫描功能可以看到当前区域的无线网络，然后选择相应的 SSID 进行连接。因此 SSID 就相当于无线网络的名称，一般情况下将 SSID 设置为具有独特意义的字符，如公司的名称等。

下面介绍如何设置 SSID 的具体操作步骤。

（1）设置无线路由器独特的 SSID。

设置无线路由器独特的 SSID 的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，单击【转到】按钮。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，单击【确定】按钮。

03 单击左侧【无线参数】➢【基本设置】选项，如图 4-23 所示，选中【开启安全设置】复选框，在【SSID 号】文本框中输入要设置的 SSID 号，本实例输入 SSID 号为“ssh”。在【频段】下拉列表中选择要使用的频段，在【模式】下拉列表中选择要使用的无线网络协议，单击【保存】按钮。



图 4-23 【无线参数】对话框



频段可以任意选择，但是在一个区域内多个 SSID 的频段不能重复，在选择模式时，如果选择 802.11g 协议则无线网络的速度最快可以达到 54Mbps，如果选择 802.11b 协议则无线网络的最快速度可以达到 11Mbps。无线路由器采用什么协议需要无线客户端的支持。

04 弹出【Windows Internet Explorer】提示对话框，单击【确定】按钮，重新启动路由器即可。

（2）客户端连接。

使用 SSID 设置的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角图标，如图 4-24 所示，会看到无线客户端自动扫描到区域内的所有无线信号，其中信号名称“ssh”就是刚才设置的无线网络的 SSID。

02 右击无线信号【ssh】，如图 4-25 所示，在弹出的快捷菜单中选择【连接】选项。



图 4-24 扫描无线信号



图 4-25 客户端连接

03 弹出【连接到网络】对话框，在【安全密钥】文本框中输入安全密钥“sushi1986”，单击【确定】按钮。

04 单击系统桌面右下角图标，如图 4-26 所示，将鼠标放在无线网络 ssh 上可以看到无线网络的连接情况。如图 4-26 所示，无线客户端已经成功连接到无线路由器。



图 4-26　客户端连接

4. 禁用 SSID 广播

SSID 就是一个无线网络的名称，无线客户端通过无线网络的 SSID 来区分不同的无线网络。为了安全，往往要求无线 AP 禁止广播该 SSID，只有知道该无线网络 SSID 的人员才可以进行无线网络连接。禁用 SSID 广播的具体操作步骤如下。

（1）设置无线路由器禁用 SSID 广播。

无线路由器禁用 SSID 广播的具体操作步骤如下。

01 IE 浏览器的地址栏中输入“http://192.168.1.1”，单击【转到】按钮。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，单击【确定】按钮。

03 设置自己无线网络的 SSID 信息，如图 4-27 所示，取消选中【允许 SSID 广播】复选框，单击【保存】按钮。

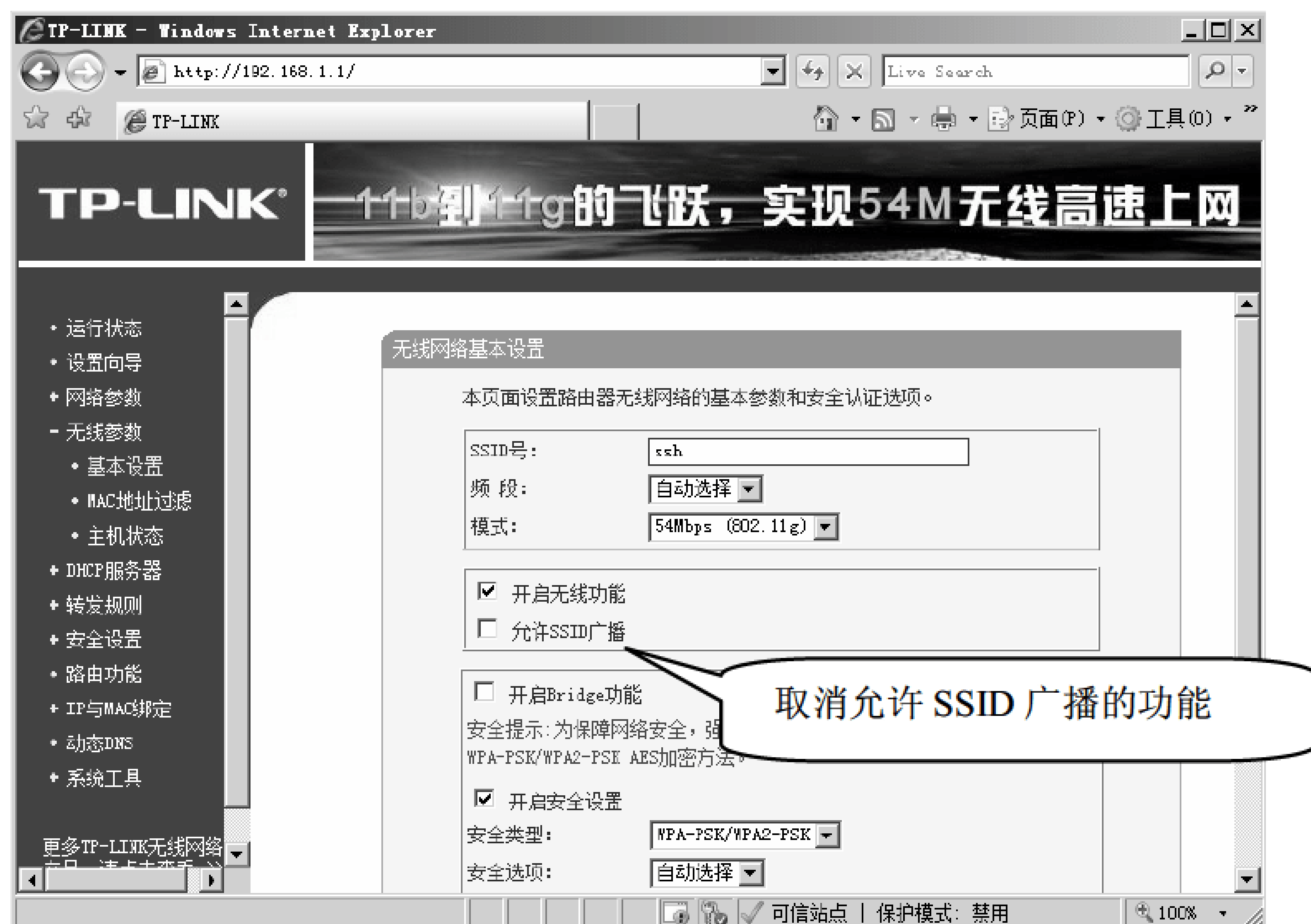


图 4-27 【无线参数】对话框

04 弹出【Windows Internet Explorer】提示对话框，单击【确定】按钮，重新启动路由器。

（2）客户端连接。

禁用 SSID 广播的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角图标，如图 4-28 所示，会看到无线客户端自动扫描到区域内的所有无线信号，会发现其中没有 SSID 为【ssh】的无线网络，但是会出现一个名称为【其他网络】的信号。

02 右击【其他网络】，如图 4-29 所示，在弹出的快捷菜单中选择【连接】选项。



图 4-28 扫描无线信号



图 4-29 客户端连接

03 弹出【连接到网络】对话框，在【名称】文本框中输入要连接网络的 SSID 号，本实例这里输入“ssh”，单击【确定】按钮。

04 在【安全密钥】文本框中输入无线网络的密钥，本实例这里输入密钥“sushi1986”，单击【确定】按钮。

05 单击系统右下角图标，如图 4-30 所示，将鼠标放在 ssh 信号上可以看到无线网络的连接情况。图 4-30 所示表明无线客户端已经成功连接到无线路由器。



图 4-30　客户端连接

5. 媒体访问控制地址过滤

网络管理的主要任务之一就是控制客户端对网络的接入和对客户端的上网行为进行控制，无线网络也不例外，通常无线 AP 利用媒体访问控制（MAC）地址过滤的方法来限制无线客户端的接入。

（1）设置无线路由器进行 MAC 地址过滤。

使用无线路由器进行 MAC 地址过滤的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，单击【转到】按钮。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，单击【确定】按钮。

03 单击左侧【无线参数】➢【MAC 地址过滤】选项，如图 4-31 所示，默认情况 MAC 地址过滤功能是关闭状态，单击【启用过滤】按钮，开启 MAC 地址过滤功能，单击【添加新条目】按钮。

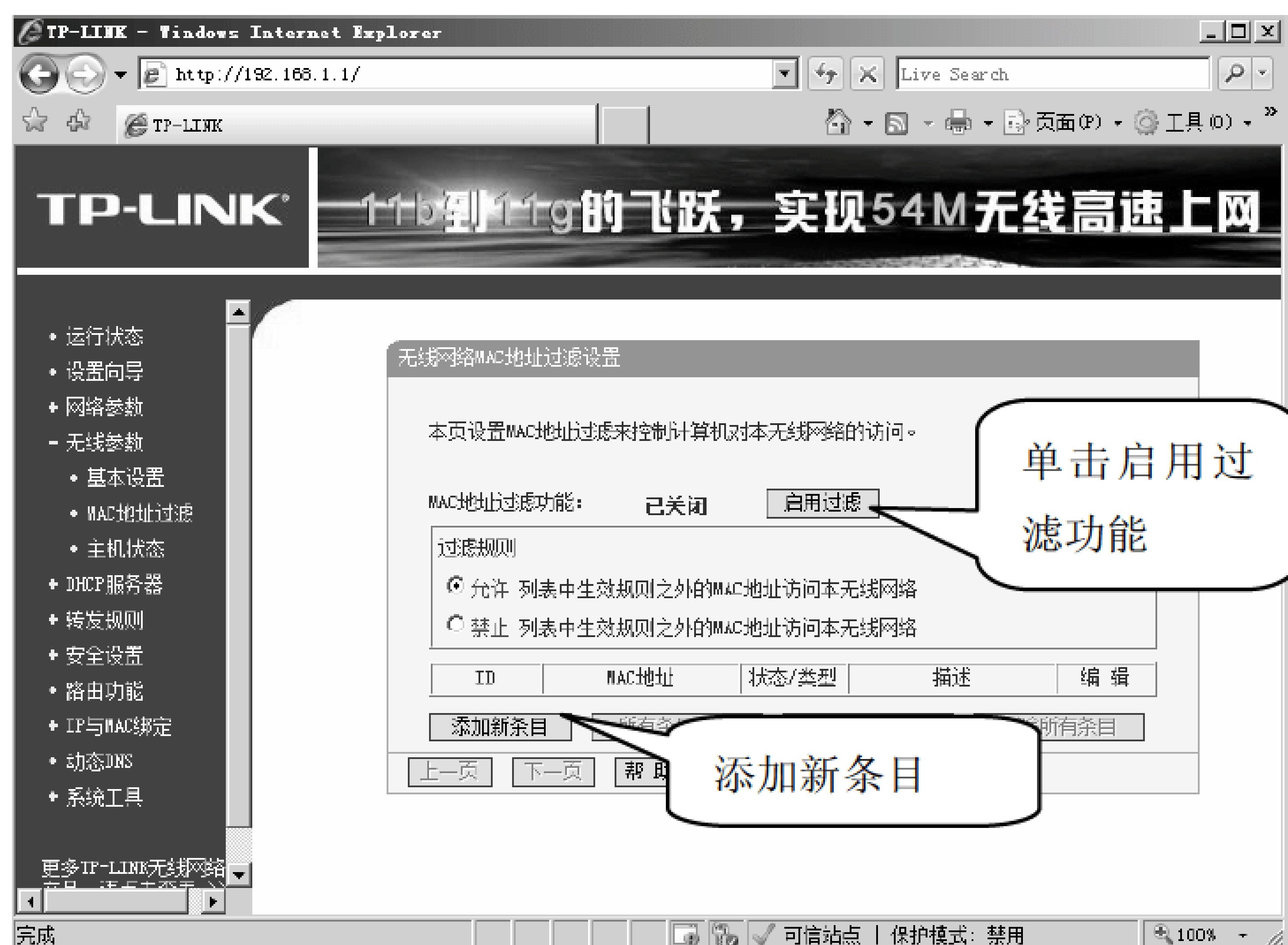


图 4-31 【无线参数】对话框

04 打开【无线网络 MAC 地址过滤设置】对话框，在【MAC 地址】文本框中输入无线客户端的 MAC 地址，如图 4-32 所示，本实例输入 MAC 地址为“00-0c-29-5A-3C-97”，在【描述】文本框中输入 MAC 描述信息“sushipc”，在【类型】下拉列表中选择【允许】选项，在【状态】下拉列表中选择【生效】选项，依照此步骤将所有合法的无线客户端的 MAC 地址加入到此 MAC 地址表后，单击【保存】按钮。



图 4-32 【无线网络 MAC 地址过滤设置】对话框

05 选中【过滤规则】选项域中的【禁止】单选按钮，如图 4-33 所示，表明在下面 MAC 列表中生效规则之外的 MAC 地址可以访问无线网络。

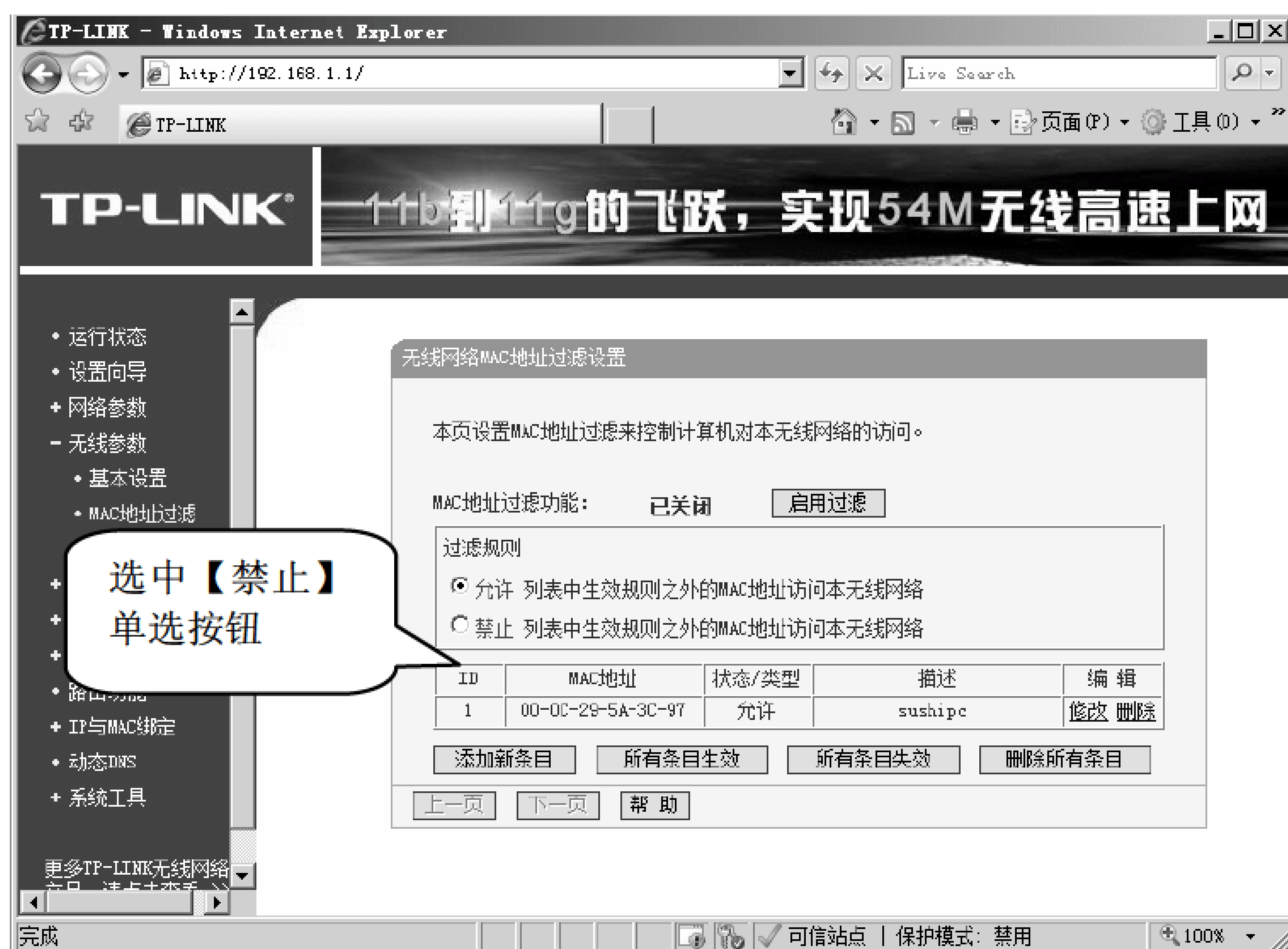


图 4-33　【过滤规则】对话框

06 弹出【Windows Internet Explorer】提示对话框，如图 4-34 所示，单击【确定】按钮，更改过滤规则。



图 4-34　【Windows Internet Explorer】提示对话框

07 客户端连接，在无线客户端访问无线 AP 时会发现除了 MAC 地址表中的 MAC 地址之外，其他的 MAC 地址无法在访问无线 AP，也就无法访问互联网。

4.3　无线网络故障诊断与排除

4.3.1　项目实战 2：无线网络连接与通信故障

（1）办公室和家中都构建了无线网络。在办公室时，笔记本计算机能够正常接入公司的无线网络；但是，回到家中后，却发现无法连接到无线网络。

故障分析：导致该故障的原因可能有以下几个。

①没有及时更改 SSID 配置。不同的无线网络使用不同的 SSID，如果 SSID 配置不正确，就无法 ping 通 AP。而且笔记本计算机将忽略该 AP，按照 SSID 配置寻找新的 AP。

②WEP 加密。如果采用的 WEP 密钥不同，无线客户端就无法与新的无线 AP 连接。如果 WEP 配置不对，无线客户端就无法从 DHCP 服务器获取 IP 地址。如果使用静态 IP 地址，无线客户端甚

至无法 ping 通 AP 的 IP 地址。

③IP 地址信息。一般情况下，无线 AP 都会自动给无线客户端分配 IP 地址，如果手工设置了无线客户端的 IP 地址，那么该客户端就将无法与新的 AP 进行通信。

故障解决：可以采用以下解决方法。

①当接入到新的无线网络时，及时更改客户端的 SSID 设置。

②如果接入无线网络需要使用密钥，则在接入该新的无线网络时，需要先获取该网络的密钥以便进行接入。

③通常情况下，使用无线 AP 分配的 IP 地址就可以了。如果要使用静态的 IP 地址，则必须确保该静态 IP 地址和无线 AP 的 IP 地址在同一网段内。

（2）按照无线网络内的其他用户进行了网络设置，包括 WEP 加密、SSID 和 IP 地址(自动获取 IP 地址)，而且无线信号显示为满格，却无法接入无线网络。

故障分析：出现这种情况，可能是网络管理员对无线 AP 设置了 MAC 地址过滤，只允许指定的 MAC 地址接入到无线网络中，而拒绝未被授权的用户，以保证无线网络的安全。

故障解决：可以与管理员联系，将你的无线网卡的 MAC 地址告诉他，让他将此 MAC 地址添加到允许接入的 MAC 地址列表中。

（3）家庭网络使用“ADSL Modem＋ 宽带路由器”的方式实现 Internet 共享，无需 PPPoE 拨号。新增的笔记本计算机无法接入到无线网络以实现 Internet 共享。

故障分析：无线 AP 一般只有一个 LAN 接口，因此，将无线 AP 接入网络时，会占用原来主机使用的网络接口，除非宽带路由器具有更多的端口，否则就无法将无线 AP 和原来的主机一同接入到宽带路由器，从而实现对 Internet 连接的共享。

故障解决：如果宽带路由器没有更多的端口可供使用，可以购买一台无线路由器，WAN 端口连接至宽带路由器，LAN 端口连接至主机，并为笔记本计算机提供无线接入。另外，也可以采用“SOHO 交换机 ＋ 无线 AP”的方式，将 SOHO 交换机连接至宽带路由器，再将无线 AP 和主机连接至 SOHO 交换机。

4.3.2　项目实战 3：无线网络共享与安全故障

（1）采用 ADSL 虚拟拨号方式上网，将无线 AP 连接至 ADSL Modem。台式机(连接无线 AP 的 LAN 端口)可以正常上网，笔记本计算机也接收到了无线信号，却无法正常上网，并且显示 IP 地址和默认网关为“不可用”。

故障分析：如果 ADSL Modem 不支持路由功能，那么使用无线 AP 就无法实现 Internet 连接共享。

故障解决：可以采取以下方法解决。

① 启用 ADSL Modem 的路由功能，实现网络连接共享。

② 购置一台无线路由器，将 LAN 连接至台式机，WAN 连接至 ADSL Modem。

③ 在台式机上安装两块网卡，并将其设置为 ICS 主机。一块网卡连接至 ADSL Modem，另一块网卡连接至无线 AP。

（2）利用无线网卡组建对等网络，两台台式机通过 ADSL 接入 Internet。先要通过无线方式将两台计算机进行连接。

故障分析及解决：方法很简单，只要购买两块无线网卡即可。将两块网卡分别安装在两台计算机中，就可以搭建起对等网络，并实现以太网的所有功能，而且可以共享上网。需要注意的是，使用这种方式时，传输速率将为 IEEE802.11b 协议理论速率(11Mb/s)的一半左右，即 6Mb/s 左右。

（3）看不到无线网络中的其他计算机，无线网卡显示正常工作，但是在网上邻居中看不到网络中的其他计算机。

故障分析及解决：

① 检查 SSID 和 WEP 参数设置，确认拼写和大小写正确无误。

② 检查计算机是否启用了文件和打印机共享，确认在无线网络属性的“常规”选项卡中“Microsoft 网络的文件和打印机共享”复选框被选中。

4.3　专家答疑

（1）为了保证无线网络标准的兼容性，在选择无线产品时，一般都会选取支持 IEEE802.11b/g 的无线 AP 和无线网卡。然而，在实际的网络测试中，发现在没有干扰和传输距离有限的情况下，无线链路的传输速率仍然较低，不能达到标称的 54Mbit/s。

答：IEEE802.11g 不但具有 54Mbit/s 的传输速率，而且，还能很好地兼容 IEEE802.11b 无线设备，从而能够将 802.11b 无线网络平滑升级到 802.11g 无线网络。

为了兼容现有的 802.11b 无线局域网设备，802.11g 除了使用和 802.11b 相同的 2.4GHz 频带外，还采用了两种不同的 OFDM（正交频分复用）编码技术，以及和相对应的 802.11b 或者 802.11g 设备通信。也就是说，在混合使用 802.11b 和 802.11g 无线设备的网络中，使用 802.11g 的无线设备既可以以 54Mbit/s 的速率和 802.11b 设备通信，也可以以 11Mbit/s 的速率和 802.11b 设备进行通信。但是，在无线局域网中，使用的是共享信道，数据链路层使用 CSMA/CA（具有冲突避免的载波帧听多路访问）来实现对无线信道的控制。也就是说，当有一台主机在和 AP 通信时，其他主机就只能处在监听状态，一旦该主机通信完毕，其他主机就会通过竞争的方式来实现对信道的控制。所以，在 802.11b 和 802.11g 混合使用的无线网络中，由于 802.11b 无法监听到 802.11g 的通信状态，就有可能在 802.11g 设备进行通信的同时抢占无线信道，从而严重干扰 802.11 设备的通信。

为了解决这一问题，802.11g 协议采用了“RTS/CTS”技术。无线局域网设备在发送数据前，都要先发送一个 RTS(Request To Send)帧给无线 AP，请求使用无线资源，如果这时 AP 没有和其他设备通信，就发送一个 CTS（Clear To Send）帧给该设备，通知它可以跟无线 AP 进行通信。这样，就避免了上述干扰问题。

（2）在构建无线时网络，怎么保证所有区域都能覆盖到，不留死角？

答：无线网络并不像有线网络那么直观，所以在布置无线网络时为了减少死角，必须要让两个 AP 覆盖的无线区域重叠，因为一个 AP 覆盖的无线网络区域一般是球形的，只有两个区域部分重叠才能确保无线信号覆盖更全面。除此之外，选择 AP 时也要考虑当前物理环境。如果是空旷的环境可以选择使用放射信号为球形的 AP 设备，如果是在大楼中的某几层可以考虑使用向某个区域放射信号的 AP 设备。

第 5 章　单机故障检测分析

局域网系统主要由硬件系统和软件系统两部分组成，因此常见的网络单机故障分为硬件故障和软件故障。本章主要介绍常见的单机故障解决思路与方案。通过本章的学习，读者可以轻松地解决常见的单机故障。

5.1　单机故障处理的基础

在处理网络单机故障之前，需要了解故障处理的基础知识。

5.1.1　硬件故障

硬件故障主要是指计算机硬件原件发生故障，而不能正常工作，一旦出现硬件故障，用户就需要及时维修，从而保证网络的正常运行。常见的硬件故障分为以下几种。

1）硬件质量问题

有些硬件故障和硬件本身的质量有关，对此用户可以更换新的硬件。

2）接触不良的故障

这类故障主要是各种板、卡、内存和 CPU 等与主板的接触不良，或电源线、数据线、音频线等的连接不良。其中各种接口卡、内存与主板接触不良的现象较为常见，用户只要更换相应的插槽位置或用橡皮擦一下金手指，即可解决这类故障。

3）参数设置错误

这类故障发生的原因是 CMOS 参数的设置问题。CMOS 参数主要有硬盘、软驱、内存的类型，以及口令、机器启动顺序、病毒警告开关等。由于参数未设置或设置不当，系统也会出现出错的警告信息提示。

4）电路故障

这类故障主要是由于主板、内存、显卡、键盘驱动器等电路芯片损坏、电阻开路，也可能是为计算机散热不良引起的硬件短路等。

5.1.2　软件故障

软件故障是指在用户使用软件的过程中出现的故障。其原因有丢失文件、文件版本不匹配、

内存冲突、内存耗尽等。常见的软件故障的表现有以下几个方面。

1）驱动程序故障

驱动程序故障可引起计算机无法正常使用。未安装驱动程序或驱动程序间产生冲突，在操作系统下的资源管理器中发现一些标记，其中“？”表示未知设备，通常是设备没有正确安装；“！”表示设备间有冲突；“×”表示所安装的设备驱动程序不正确。

2）重启或死机

运行某一软件时，系统自动重新启动或死机，只能按机箱上的重启键才能够重新启动计算机。

3）提示内存不足

在软件的运行过程中，提示内存不足，不能保存文件或某一功能不能使用。这种现象经常出现在图像处理软件中，例如 Photoshop CS5、AutoCAD 2012 等软件。

4）运行速度缓慢

在计算机的使用过程中，当用户打开多个软件时，计算机的速度明显变慢，甚至出现假死机的现象。

5）软件中毒

病毒对计算机的危害是众所周知的，轻则影响机器速度，重则破坏文件或造成死机。一旦病毒感染了软件，就可以在后台启动软件，甚至破坏软件的文件，导致软件无法使用。

5.2 单机故障产生的原因

计算机故障产生的原因很多，大致上可以分为硬件引起故障和软件引起故障。

1. 硬件产生故障

计算机的硬件故障主要是指物理硬件的损坏、CMOS 参数设置不正确、硬件之间不兼容等引起的计算机不能正常使用的现象。硬件故障产生的原因主要来自于内存不兼容或损坏、CPU 针脚问题、硬盘损坏、机器磨损、静电损坏、用户操作不当和外部设备接触不良等。

虽然硬件故障产生的原因很多，但归纳起来有以下几种。

1）非正常使用

当计算机出现故障时，如果用户在机器运行的情况下乱动机箱内部的硬件或连线，很容易造成硬件的损坏。例如，当系统在运行时，如果用户直接把硬盘卸掉，很容易直接造成数据的丢失，或者造成硬盘的物理坏道，这主要是因为硬盘此时正在高速运转。

2）硬件的不兼容

硬件之间在相互搭配工作的时间，需要具有共同的工作频率。同时由于主板对各个硬件的支持范围不同，所以硬件之间的搭配很重要。例如，在升级内存时，如果主板不支持，将造成无法开机的故障。如果插入两个内存，就需要尽量让它们是同一型号的产品，否则也会出现这样或那样的硬件故障现象。

3）灰尘太多

灰尘一直是硬件的隐形杀手，机器内灰尘过多会引起硬件故障。例如，软驱磁头或光驱激光头沾染过多灰尘后，会导致读写错误，严重的会引起计算机死机。另外对于潮湿天气还会造成电路短路现象，灰尘对计算机的机械部分也有极大影响，造成运转不良，从而不能正常工作。

4）硬件和软件不兼容

每一个版本的操作系统或软件都会对硬件有一定的要求，如果不能满足要求，也会产生计算机故障。例如一些三维软件和特殊软件，由于对内存的需要比较大，当内存较小时，系统会出现死机等故障现象。

5）CMOS 设置不当

CMOS 设置的有关参数需要和硬件本身相符合。如果设置不当，会造成系统故障。例如，硬盘参数、模式或内存参数设置不当会导致计算机无法启动。又例如，将无 ECC 功能的内存设置为具有 ECC 功能，这样就会因内存错误而造成死机。

6）周围的环境

计算机周围的环境主要包括电源、温度、静电和电磁辐射等因素的影响。过高过低或忽高忽低的交流电压，都将对计算机系统造成很大危害。如果计算机的工作环境温度过高，对电路中的元器件影响最大，首先会加速其老化损坏的速度，其次过热会使芯片插脚焊点脱焊。由于目前计算机采用的芯片仍为 CMOS 电路，从而环境静电会比较高，这样很容易造成计算机内部硬件的损坏。另外，电磁辐射也会造成计算机系统的故障，所以计算机应该远离冰箱、空调等电气设备，不要与这些设备共用一个插座。

2. 软件引起的故障

软件在安装、使用和卸载的过程中也会引起故障，主要原因有以下几个方面。

1）系统文件误删除

由于 Windows 操作系统启动需要有 Command.com、Io.sys、Msdos.sys 等文件，如果这些文件遭到破坏或被误删除，会引起计算机不能正常使用。

2）病毒感染

计算机感染病毒后，会出现很多种故障现象，如显示内存不足、死机、重启、速度变慢、系统崩溃等现象。这时用户可以使用杀毒软件（如 360 杀毒、金山毒霸、瑞星等）来进行全面查毒和杀毒，并做到定时升级杀毒软件。

3）动态链接库文件丢失

在 Windows 操作系统中还有一类文件也相当重要，这就是扩展名为 DLL 的动态链接库文件，这些文件从性质上来讲是属于共享类文件，也就是说，一个 DLL 文件可能会有多个软件在运行时需要调用它。如果用户在删除一个应用软件的时候，该软件的反安装程序会记录它曾经安装过的文件并准备将其逐一删去，这时候就容易出现被删掉的动态链接库文件同时还会被其他软件用到的情形，如果丢失的链接库文件是比较重要的核心链接文件的话，那么系统就会死机，甚至崩溃。

4）注册表损坏

在操作系统中，注册表主要用于管理系统的软件、硬件和系统资源。用户操作不当、黑客的攻击、病毒的破坏等会造成注册表的损坏，也会造成计算机故障。

5）软件升级故障

大多数人可能认为软件升级是不会有问题的，事实上在升级过程中也会对其中共享的一些组件进行升级，但是其他程序可能不支持升级后的组件从而造成计算机故障。

6）非法卸载软件

不要把软件安装所在的目录直接删掉，如果直接删掉的话，注册表和 Windows 目录中会有很多垃圾存在，时间长了，系统也会不稳定，从而产生计算机故障。

5.3 故障诊断的原则和方法

了解了故障处理的基础知识后，下面继续学习故障诊断的原则和方法。

5.3.1 单机故障诊断的原则

用户要想更快更好地排除计算机故障，就必须遵循一定的原则。下面将介绍常见的故障诊断原则。

1. 先假后真

计算机故障有真故障和假故障两种。在发现计算机故障时首先要确定是否为假故障，仔细观察计算机的环境，是否有其他电器的干扰，设备之间的连线是否正常，电源开关是否打开，自己的操作是否正确等，排除了假故障之后，方可进行真故障的诊断与修理。

2. 先软后硬

所谓先软后硬诊断原则，是指在诊断的过程中，先判断是否为软件故障，当软件没有任何问题时，如果故障不能消失，再从硬件方面着手检查。

3. 先外后内

对于故障涉及外部设备时，应先检查机箱和显示的外部件，特别是机箱外的一些开关、旋钮是否调整外部的引线、插座有无断路、短路现象等，实践证明许多用户的计算机故障都是由此而起的。当确认外部设备正常时，再打开机箱或显示设备进行检查。

4. 先简单后复杂

在进行计算机故障诊断的过程中，应先进行简单的检查工作，如果还不能消除故障，再进行那些相对比较复杂的工作。

所谓简单的事情，是指对计算机的观察和周围环境的分析。观察具体包含以下几个方面。

（1）计算机周围的环境情况，包括位置、电源、连接、其他设备、温度与湿度等。

（2）计算机所表现的现象、显示的内容，以及它们与正常情况下的异同。

（3）计算机内部的环境情况，包括灰尘、连接、器件的颜色、部件的形状、指示灯的状态等。

（4）计算机的软硬件配置，包括安装了什么硬件，资源的使用情况，使用的是哪个版本的操作系统，安装了什么应用软件，硬件的设置驱动程序版本等。

用户需要观察的简洁的环境包括以下几个方面。

（1）首先判断在最小系统下计算机是否正常。

（2）判断没有问题的部件是什么，怀疑的部件是什么。

（3）在一个干净的系统中，添加用户的硬件和软件来进行分析判断。

从简单的事情做起，有利于精力的集中和进行故障的判断与定位。所以用户需要通过认真的观察后，才可进行判断与维修。

5. 先一般后特殊

遇到计算机的故障时，用户首先需要考虑带有普遍性和规律性的常见故障，最常见的原因是什么，如果这样还不能解决问题，再考虑比较复杂的原因。这样便于逐步缩小故障范围，由面到点，缩短修理时间。例如，计算机启动后显示器灯亮，但不显示图像，此时用户应该先查看显示器的数据线是否连接正常，或者换个数据线试试，也许这样就可以解决问题。

5.3.2 单机故障诊断的方法

掌握好故障诊断的原则后，下面将介绍几种故障的诊断方法。

1. 查杀病毒法

病毒是引起计算机故障的常见因素，此时用户可以使用杀毒软件进行杀毒以解决故障问题。常用的杀毒软件包括 360 杀毒、瑞星、金山毒霸、NOD32 等，利用这些软件先进行全盘扫描，发现病毒后及时查杀，如果没有发现病毒，可以升级一下病毒库。查杀病毒法在解决计算机故障时是用户首先需要考虑的方法，这样可以使用户少走很多弯路。

2. 清洁硬件法

对于长期使用的计算机，一旦出现故障，用户就需要考虑灰尘的问题。因为长时间的灰尘积累，会影响计算机的散热，从而引起计算机故障，所有用户需要保持计算机清洁。同时还要查看主板上的引脚是否有发黑的现象，这是引脚被氧化的表现，一旦引脚被氧化，很有可能导致电路接触不良，从而引起计算机故障。

在清洁硬件的过程中，应注意以下几个方面的事项。

（1）注意风扇的清洁。包括 CPU 风扇、电源风扇和显卡风扇等。在清洁风扇的过程中，最好能在风扇的轴处涂抹一点钟表油，加强润滑。

（2）注意风道的清洁。在机箱的通风处清洗，保证通风畅通性。

（3）注意插头、座、槽、板卡金手指部分的清洁。对于金手指的清洁，用户可以用橡皮擦拭金手指部分，或用酒精棉擦拭也可以。插头、座、槽的金属引脚上的氧化现象的去除方法：采用橡皮擦或专业的清洁剂清除表面的氧化层即可。

（4）大规模集成电路、元器件等引脚处的清洁。清洁时，应用小毛刷或吸尘器等除掉灰尘，同时要观察引脚有无虚焊和潮湿的现象，元器件是否有变形、变色或漏液现象。

（5）注意使用的清洁工具。清洁用的工具，首先是防静电的。如清洁用的小毛刷，应使用天然材料制成的毛刷，禁用塑料毛刷。其次是如使用金属工具进行清洁时，必须切断电源，且对金属工具进行释放静电的处理。

（6）对于比较潮湿的情况，应想办法使其干燥后再使用。可用的工具如电风扇、电吹风等，也可让其自然风干。

3. 直接观察法

直接观察法可以总结为“望闻听切”4 个字，具体方法如下。

（1）望。观察系统板卡的插头、插座是否歪斜，电阻、电容引脚是否相碰，表面是否烧焦，芯片表面是否开裂，主板上的铜箔是否烧断。还要查看是否有异物掉进主板的元器件之间(造成短路)，也可以看看板上是否有烧焦变色的地方，印刷电路板上的走线(铜箔)是否断裂等。

（2）闻。闻主机、板卡中是否有烧焦的气味，便于发现故障和确定短路所在地。

（3）听。即监听电源风扇、软/硬盘电机或寻道机构、显示器变压器等设备的工作声音是否正常。另外，系统发生短路故障时常常伴随着异常声响。监听可以及时发现一些事故隐患和帮助在事故发生时即时采取措施。

（4）切。即用手按压管座的活动芯片，看芯片是否松动或接触不良。另外，在系统运行时用手触摸或靠近 CPU、显示器、硬盘等设备的外壳根据其温度可以判断设备运行是否正常；用手触摸一些芯片的表面，如果发烫，则为该芯片损坏。

4. 替换法

替换法是用好的部件去代替可能有故障的部件，以判断故障现象是否消失的一种维修方法。好的部件可以是同型号的，也可能是不同型号的。替换的顺序一般为以下 4 个步骤。

（1）根据故障的现象或第二部分中的故障类别，来考虑需要进行替换的部件或设备。

（2）按先简单后复杂的顺序进行替换。如先内存、CPU，后主板；如要判断打印故障时，可先考虑打印驱动是否有问题，再考虑打印电缆是否有故障，最后考虑打印机或并口是否有故障等。

（3）最先检查与怀疑有故障的部件相连接的连接线、信号线等，接着替换怀疑有故障的部件，然后替换供电部件，最后是与之相关的其他部件。

（4）从部件的故障率高低来考虑最先替换的部件。故障率高的部件先进行替换。

5. 插拔法

插拔法包括逐步添加和逐步去除两种方法。

逐步添加法，以最小系统为基础，每次只向系统添加一个部件/设备或软件，来检查故障现象是否消失或发生变化，以此来判断并定位故障部位。

逐步去除法，正好与逐步添加法的操作相反。

逐步添加/去除法一般要与替换法配合，才能较为准确地定位故障部位。

6. 最小系统法

最小系统是指，从维修判断的角度能使计算机开机或运行的最基本的硬件和软件环境。最小系统有两种形式。

硬件最小系统：由电源、主板和 CPU 组成。在这个系统中，没有任何信号线的连接，只有电源到主板的电源连接。在判断过程中是通过声音来判断这一核心组成部分是否可正常工作。

软件最小系统：由电源、主板、CPU、内存、显示卡/显示器、键盘和硬盘组成。这个最小系统主要用来判断系统是否可完成正常的启动与运行。

对于软件最小系统，有以下几点需要说明。

（1）硬盘中的软件环境，保留着原先的软件环境，只是在分析判断时，根据需要进行隔离（如卸载、屏蔽等）。保留原有的软件环境，主要是用来分析判断应用软件方面的问题。

（2）硬盘中的软件环境，只有一个基本的操作系统环境，可能是卸载掉所有应用，或是重新安装一个干净的操作系统，然后根据分析判断的需要，加载需要的应用。需要使用一个干净的操作系统环境，主要是判断系统问题、软件冲突或软、硬件间的冲突问题。

（3）在软件最小系统下，可根据需要添加或更改适当的硬件。如：在判断启动故障时，由于硬盘不能启动，想检查一下能否从其他驱动器启动。这时，可在软件最小系统下加入一个软驱或干脆用软驱替换硬盘来检查。又如：在判断音视频方面的故障时，应需要在软件最小系统中加入声卡；在判断网络问题时，就应在软件最小系统中加入网卡等。

最小系统法，主要是要先判断在最基本的软、硬件环境中，系统是否可正常工作。如果不能正常工作，即可判定最基本的软、硬件部件有故障，从而起到故障隔离的作用。

最小系统法与逐步添加法结合，能较快速地定位发生在其他部件或软件的故障，提高维修效率。

7. 程序测试法

随着各种集成电路的广泛应用，焊接工艺越来越复杂，同时，随机硬件技术资料较缺乏，仅硬件维修手段往往很难找出故障所在。而通过随机诊断程序、专用维修诊断卡以及根据各种技术参数（如接口地址），自编专用诊断程序来辅助硬件维修则可达到事半功倍之效。

程序测试法的原理就是用软件发送数据、命令，通过读线路状态和某个芯片（如寄存器）状态来识别故障部位。此法往往用于检查各种接口电路故障以及具有地址参数的各种电路。但此法应用的前提是 CPU 及总线基本运行正常，能够运行有关诊断软件，能够运行安装于 I/O 总线插槽上的诊断卡等。编写的诊断程序要严格、全面、有针对性，能够让某些关键部位出现有规律的信号，能够对偶发故障进行反复测试以及显示记录出错情况。软件诊断法要求具备熟练编程技巧，熟悉各种诊断程序与诊断工具（如 debug、DM 等），掌握各种地址参数（如各种 I/O 地址）及电路组成原理等，尤其掌握各种接口单元正常状态的各种诊断参考值是有效运用软件诊断法的前提基础。

8. 对比检查法

对比检查法与替换法类似，即用好的部件与怀疑有故障的部件进行外观、配置、运行现象等方面的比较，也可在两台计算机间进行比较，以判断故障计算机在环境设置、硬件配置方面的不同，从而找出故障部位。

5.4　常见硬件故障分析及解决方案

本节主要讲述硬件分析及解决方案。

5.4.1　常见 CPU 故障现象及解决方案

下面就 CPU 引起的问题介绍几种常见故障的解决方案。

1. 开机无反应

【故障表现】：一台计算机在经过一次挪动后，按下电源开关，开机系统无任何反应，电源风扇不转，显示器无任何显示，机箱的喇叭无任何声音。

【故障诊断】：由于计算机经过了挪动，说明机箱内部的硬件出现了接触不良的故障。首先打开机箱，看一下风扇是否被堵住，检查下显卡是否松动，拔下显卡后用橡皮擦下，然后再重新插到主板上，开机检测，如果还是无反应，开始检查 CPU 的问题。关闭电源，将 CPU 拔下，发现 CPU 有松动，而且 CPU 的针脚有发绿的现象，表示 CPU 被氧化了。

【故障处理】：卸下 CPU，用皮老虎清理一下 CPU 插槽，然后用橡皮擦清理一下针脚，重新插上 CPU，通电开机，计算机恢复正常。

2. 针脚损坏

【故障表现】：一台计算机运行正常，为了散热，用户卸下 CPU，涂抹一些散热胶，然后重新插上 CPU，按下电源开关后，不能开机。

【故障诊断】：因为用户只是将 CPU 拆下涂抹了些散热胶，并没有做太大的改动，所以首先想到是某个部件接触不良，或者灰尘过多造成的。首先将显卡、内存等部件全部去掉，进行简单的清理工作，然后将主板上的灰尘也打扫干净。重新安装后问题依然存在，然后想到 COMS 电池没电也会引发无法开机的问题，于是换了一颗新的电池，可是依然无法开机。此时根据先前做的操作，可以将 CPU 拆下，观察发现插座内数个针脚已经变形，而且还有一个针脚断了，如图 5-1 所示。

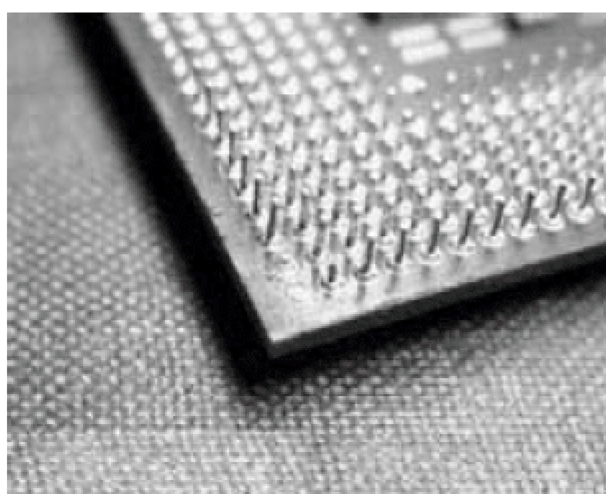


图 5-1　针脚损坏的 CPU

【故障处理】：根据故障诊断，可以判断是针脚的问题，先用镊子将针脚复位，然后将断的针脚焊接上。安装上 CPU，重新开机测试，问题解决。具体焊接的操作步骤如下。

01 首先将 CPU 断脚处的表面刮净，用焊锡和松香对其迅速上锡，使焊锡均匀地敷在断面上即可。



图 5-2　焊接后的 CPU 针脚

02 将 CPU 断脚刮净，用同样的方法上锡。如果短脚丢失，可以找个大头针代替。

03 用双面胶将 CPU 固定在桌面上，左手用镊子夹住断脚，使上锡的一端与 CPU 断脚处相接，右手用电烙铁迅速将两者焊接在一起，可多使用一些松香，使焊点细小而光滑，如图 5-2 所示。

04 将 CPU 小心地插入 CPU 插座内，如果插不进去，可用刀片对焊接处小心修整，插好后开机测试。

3. CPU 温度过高导致系统关机重启

【故障表现】：一台计算机使用一段时间后，会自动关机并重新启动系统，然后过几分钟又关机重启，此现象反复发生。

【故障诊断】：首先用杀毒软件进行全盘扫描杀毒，如果没有发现病毒，则关闭电源，打开机箱，用手摸下 CPU，发现很烫手，说明温度比较高，而 CPU 的温度过高会引起不断重启的现象。

【故障处理】：解决 CPU 温度高引起的故障的具体操作步骤如下。

01 打开机箱，开机并观察计算机自动关机时，发现 CPU 的风扇停止转动，然后关闭电源，将风扇拆下，用手转下风扇，风扇转动很困难，说明风扇出了问题。

02 使用软毛刷将风扇清理干净，重点清理风扇转轴的位置，并在该处滴几滴润滑油，经过处理后试机。如果故障依然存在，可以换个新的风扇，再次通电试机，计算机运行正常，故障排除。

03 为了更进一步提高 CPU 的散热能力，可以除去 CPU 表面旧的硅胶，重新涂抹新的硅胶，这样也可以加快 CPU 的散热，提高系统的稳定性。

04 检查计算机是否超频。如果计算机超频工作，会带来散热问题。用户可以使用鲁大师检查一下计算机的问题，如果是因为超频带来的高温问题，可以重新设置 COMS 的参数。计算机温度检测如图 5-3 所示。



图 5-3　计算机温度检测

5.4.2 常见内存故障现象及解决方案

下面就内存引起的问题介绍几种常见故障的解决方法。

1. 开机长鸣

【故障表现】：计算机开机后一直发出“嘀，嘀，嘀”的长鸣，显示器无任何显示。

【故障诊断】：从开机后计算机一直长鸣可以判断出是硬件问题，根据声音的间断为一声，可以判断为内存问题。关机后拔下电源，打开机箱并卸下内存条，仔细观察发现内存的金手指表面覆盖了一层氧化膜，而且主板上有很多灰尘。因为机箱内的湿度过大，内存的金手指发生了氧化，从而导致内存的金手指和主板的插槽之间接触不良，而且灰尘也是导致原件接触不良的常见因素。

【故障处理】：排除该故障的具体操作步骤如下。

01 关闭电源，取消内存条，用皮老虎清理一下主板上内存插槽。

02 用橡皮擦一下内存条的金手指，将内存插回主板的内存插槽中。在插入的过程中，双手拇指用力要均匀，将内存压入到主板的插槽中，当听到“啪”的一声表示内存已经和内存卡槽卡好，内存成功安装。内存插入方法如图 5-4 所示。

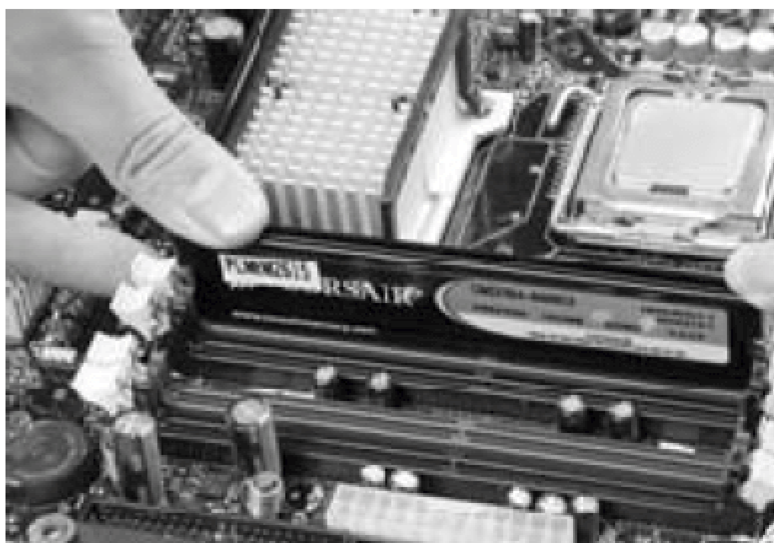


图 5-4　内存插入方法

03 接通电源并开机测试，计算机成功自检并进入操作系统，表示故障已排除。

2. 提示内存写入错误

【故障表现】：一台旧计算机，最近在使用的时候突然弹出提示【“0x7c9301b3”指令引用的“0x74e51782”的内存，该内存不能为“written”】，单击【确定】按钮后，打开的软件自动关闭，计算机死机，如图 5-5 所示。

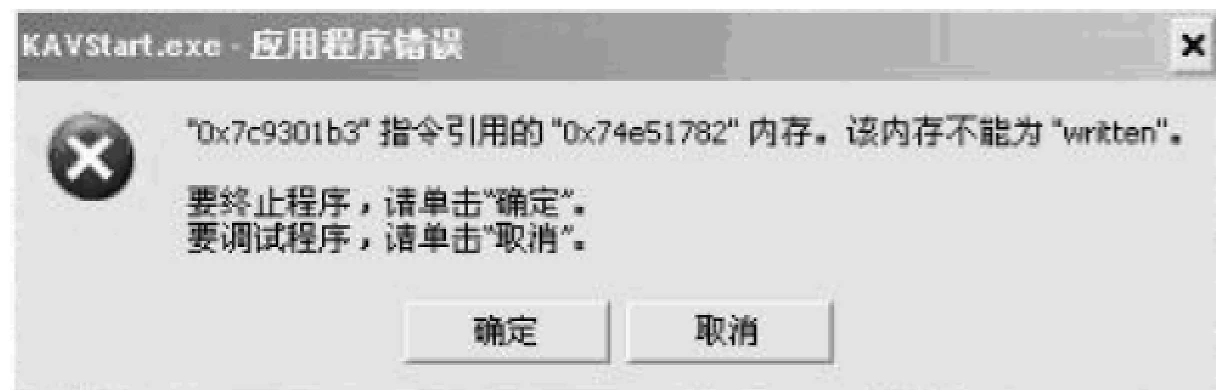


图 5-5　内存写入错误提示

【故障诊断】：上诉提示表面故障的原因与内存有一定的关系。但是内存是不容易坏的原件，所以用户应该采用【先软后硬】的原则进行排除问题。

【故障处理】：排除该故障的具体操作步骤如下。

01 使用杀毒软件检查系统中是否有木马或病毒。这类程序为了控制系统往往任意篡改系统文件，从而导致操作系统异常。用户平常应加强信息安全意识，对来源不明的可执行程序要使用杀毒软件检测一下。查杀完病毒后没有发现病毒。

02 更换正版的应用程序，有些应用程序存在一定的漏洞，也会引起上述故障。重新安装应用程序后故障依然存在。

03 重装操作系统。如果用户使用的是盗版的操作系统，也会引起上述故障。重新安装操作系统后，故障排除，说明故障与操作系统有关。

【备用处理方案】：如果故障还不能排除，可以从硬件下手查看故障的原因，具体操作步骤如下。

01 打开机箱，查看内存插在主板上的金手指部分灰尘是否较多，硬件接触不良也会引起上述故障。用橡皮擦一下内存的金手指两侧，然后用皮老虎清理一下内存插槽。清理完成后，重新插上内存。

02 使用替换法检查是否是内存本身的质量问题。如果内存有问题，可以更换一条新的内存条。

03 从内存的兼容性下手，检查是否存在不兼容问题。使用不同品牌、不同容量或者不同工作频率参数的内存，也会引起上述故障。可以更换内存条以解决故障。

3. 内存损坏导致系统经常报告注册表错误

【故障表现】：一台计算机能够正常启动，但是进入系统桌面时，系统会提示注册表读取错误，需要重新启动计算机修复该错误。重新启动点后故障依然存在。

【故障诊断】：系统提示注册表读取错误，因而用户可先从注册表的修复下手，在安全模式下禁用部分启动项。

【故障处理】：排除该故障的具体操作步骤如下。

01 重新启动计算机，并按【F8】功能键进入【Windows 高级启动选项】界面，然后选择【安全模式】选项，按【Enter】键进入系统的安全模式，如图 5-6 所示。

02 单击【开始】按钮，在弹出的【开始】菜单中选择【所有程序】➤【附件】➤【运行】命令，如图 5-7 所示。



图 5-6 【Windows 高级启动选项】界面



图 5-7 【开始】菜单

03 弹出【运行】对话框，在【打开】文本框中输入“msconfig”，单击【确定】按钮，如图 5-8 所示。

04 弹出【系统配置实用程序】对话框，选择【启动】选项卡，取消列表中的所有复选框，即禁用所有启动项，单击【确定】按钮，如图 5-9 所示。



图 5-8 【运行】对话框



图 5-9 【系统配置实用程序】对话框

05 弹出提示对话框，单击【重新启动】按钮，计算机将重新启动，再次进入操作系统故障排除，如图 5-10 所示。

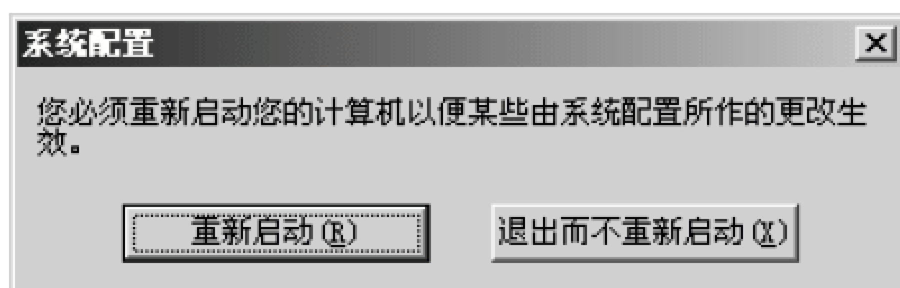


图 5-10 系统重新启动提示对话框

【备用处理方案】：经过上述操作后，如果故障依然存在，基本上可以判定是内存本身存在问题，此时采用替换法，换上一个性能良好的内存条，即可解决上述故障。

5.4.3 常见硬盘故障现象及解决方案

硬盘的硬故障也就是指硬盘电路板损坏、盘片划伤、磁头组件损坏等故障。剧烈的震动、频繁开关机、电路短路、供电电压不稳定等比较容易引发硬盘物理性故障。由于这种情况的故障维修对维修条件和维修设备要求较高，一般无法自行维修，所以需要由专业技术人员才能解决。用户千万不要盲目拆盖、拔插控制卡或轻易将硬盘进行低级格式化，使问题变得更加复杂化。有时还会由于维护操作不当，不仅没有把故障修复好，反而引起新的故障。图 5-11 所示为硬盘结构。

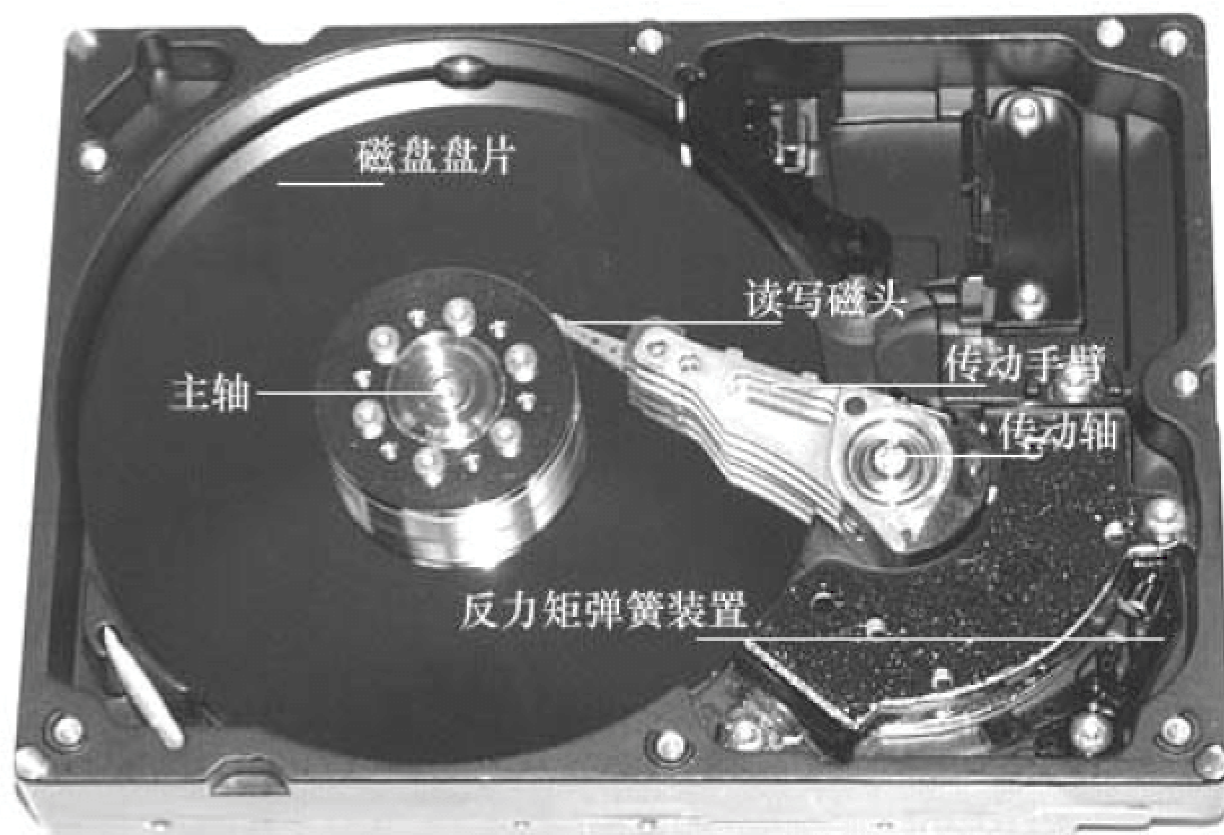


图 5-11　硬盘结构

硬盘实体未发生损坏只是逻辑数据故障，可使用软件进行修复，这类硬盘故障称为“逻辑故障”。硬盘逻辑故障相对于物理故障更容易修复些，而对数据的损坏程度也比物理故障轻些。

1. 在 Windows 初始化时死机

【故障表现】：计算机开机自检时停滞不前且硬盘和光驱的灯一直常亮不闪。

【故障分析】：出现这种现象的原因是由于系统启动时，从 BIOS 启动然后再去检测 IDE 设备，系统一直检查，而设备未准备好或根本就无法使用，这时就会造成死循环，从而导致计算机无法正常启动。

【故障处理】：用户应该检查硬盘数据线和电源线的连接是否正确或是否有松动，让系统找到硬盘，就可解决此问题。

2. 分区表遭到破坏

【故障表现】：计算机开机时出现提示信息【Invalid Partition Table】，然后无法正常启动系统。

【故障分析】：该信息表示计算机中存在无效分区表，该故障现象出现的原因有两个：一是分区表错误引发的启动故障，二是分区有效标志错误的故障。

【故障处理】：根据不同的情况，设置不同的排除方法。

1）分区表错误引发的启动故障

分区表错误是硬盘的严重错误，不同的错误程序会造成不同的损失。如果没有活动分区标志则计算机无法启动。但从软驱或光驱引导系统后，可对硬盘读写，通过 FDISK 命令重置活动分区进行修复。如果某一分区类型错误可造成某一分区丢失。分区表的第四个字节为分区类型值，正常可引导的大于 32MB 的基本 DOS 分区值为 06，而扩展 DOS 分区值是 05。利用此类型值可实现单个分区的加密技术，恢复原正确类型值即可使该分区恢复正常。

用户遇到此类故障，可用硬盘维护工具 NU 等工具软件修复检查分区表中的错误，若发现错误将会询问是否愿意修改，只要不断回答“YES”即可修正错误（或用备份过的分区表覆盖）。如果由于病毒感染了分区表，即使高级格式化也解决不了问题，可先用杀毒软件杀毒，再用硬盘维护工具进行修复。

2）分区有效标志错误的故障

在硬盘主引导扇区中最后两个字节 55AA 为扇区的有效标志。当从硬盘、软盘或光盘启动时将检测这两个字节，如果存在则认为硬盘存在，否则将不承认硬盘。

此类故障的解决方法是：采用 DEBUG 方法进行恢复处理。当 DOS 引导扇区无引导标志时，系统启动将显示为 Missing Operating System。这时，可从软盘或光盘引导系统后使用“SYS C:”命令传送系统修复故障，包括引导扇区和系统文件都可自动修复到正常状态。

3）硬盘的逻辑坏道

硬盘逻辑坏道故障的表现如下。

（1）在读取某一文件或运行某一程序时，硬盘反复读盘且经常出错，提示文件损坏等信息，或者要经过很长时间才能成功，并在读盘的过程中不断发出刺耳的杂音。一旦出现这种现象，就表明硬盘上的某些扇区已经损坏。

（2）Windows 中的 SCANDISK 功能可以在开机时对硬盘实现自动监测并修复硬盘上的逻辑坏道。如果每次启动 Windows 系统都会自动运行 SCANDISK 扫描磁盘错误进行自检，有时还不能通过自检，这时就可以判定硬盘上已经存上坏道。

（3）在用 FDisk 分区时，FDisk 会对每一分区中的扇区进行检测，如果发现有扇区损坏，FDisk 的检测进度就会反反复复，如 FDisk 已经检测了一半，又会从头开始检测，如此这样反复进行。这种现象就意味着该硬盘有坏道。

（4）开机时系统不能通过硬盘引导，软盘启动后可以转到硬盘盘符，但无法进入，用 SYS 命令传导系统也不能成功。这种情况比较严重，很有可能是硬盘的引导扇区出了问题。

（5）在用 FORMAT 格式化硬盘时，到某一进度停止不前，最后报错，无法完成。这也说明硬盘中存上坏道。因为在用 FORMAT 格式化硬盘某一分区时，FORMAT 会以簇为单位对分区进行检测。若某一簇中有坏扇区存在，该簇即为坏簇。FORMAT 发现后就会试图进行修复，在修复的过程中进度会停滞不前。

（6）正常使用计算机时，会频繁无故地出现蓝屏、死机的现象。这也是由于硬盘扇区上的数据信息被损坏而造成系统程序出错引起的，是一种比较常见的现象。

上述故障都是用户会经常遇到的，也是一些非常典型的硬盘坏道故障。一些普通的硬盘修复工具都可处理逻辑坏道，遇到这类故障用户不必心慌。

（1）使用 Windows 自带的 SCANDISK 工具修复。SCANDISK 工具只能修复逻辑坏道，对于物理坏道则无能为力。启动 SCANDISK 工具后会自动对硬盘上的逻辑坏道进行修复，即使用户在 Windows 操作过程中非正常关机，当再启动 Windows 时 SCANDISK 仍会自动启动以修复硬盘上的逻辑坏道，就好像有记忆功能，给用户带来极大方便。另外，在 DOS 状态下，也可启动 SCANDISK 工具进行全盘扫描和修复。

（2）使用低级格式化软件修复。将硬盘低级格式化操作后，硬盘所有扇区的伺服信息和校验信息都将被重写，数据区也全部归零。硬盘的逻辑坏道其实就是磁盘扇区上校验信息（ECC）与磁道的数据和伺服信息不匹配，低级格式化后这些不匹配信息也都被全部归零，这样逻辑坏道就不存在了。至于可以对硬盘低级格式化的软件有多种，如 DM、Lformat 等。

（3）使用清零软件修复。使用清零软件将硬盘扇区中的数据区全部清零也可修复逻辑坏道，

这种方法的操作和对硬盘进行低级格式化操作基本相同。可对硬盘清零的软件有多种，如 MHDD、DM 软件，其中使用 MHDD 中的清零功能是一种比较典型的方法。

3. 磁盘碎片过多，导致系统运行缓慢

计算机使用一段时间后，速度就会变慢，除了系统本身的原因以外，磁盘中产生文件碎片也是一个重要的原因。

由于硬盘被划分成一个一个簇，然后里头分成各个扇区，文件的大小不同，在存储的时候系统会搜索相应的大小，久而久之在文件和文件之间会形成一些碎片，较大的文件也可能被分散存储；产生碎片以后，在读取文件时需要更多的时间查找，从而减慢操作速度，对硬盘也有一定损害，因此过一段时间应该进行一次碎片整理。

5.4.4 常见显卡故障及解决方案

网卡又称为网络接口卡，是计算机连入互联网的必要设备。一旦网卡出现故障，计算机就不能上网。

1. 开机无显示

【故障表现】：启动计算机时，显示器出现黑屏现象，而且机箱喇叭发出一长两短的报警声。
【故障分析】：从故障可以看出很可能是显卡引发的故障。
【故障排除】：主要从以下几个方面着手检查。

（1）判断是否由于显卡接触不良引发的故障。关闭电源，打开机箱，将显卡拔出来，然后用毛笔刷将显卡板卡上的灰尘清理掉，特别是要注意将显卡风扇及散热片上的灰尘处理掉。接着用橡皮擦来回擦拭板卡的金手指。完成这一步之后，将显卡重新安装好，查看故障是否已经排除。

（2）针对接触不良的显示卡，比如一些劣质的机箱背后挡板的空档不能和主板 AGP 插槽对齐，在强行上紧显示卡螺丝以后，过一段时间可能导致显示卡的 PCB 变形的故障，只要尝试着松开显示卡的螺丝即可。如果使用的主板 AGP 插槽用料不是很好，AGP 槽和显示卡 PCB 不能紧密接触，用户可以使用宽胶带将显示卡挡板固定，把显示卡的挡板夹在中间。

（3）检查显示卡金手指是否已经被氧化，使用橡皮清除锈渍显示卡后仍不能正常工作的话，可以使用除锈剂清洗金手指，然后在金手指上轻轻地敷上一层焊锡，以增加金手指的厚度，但一定注意不要让相邻的金手指之间短路。

（4）检查显卡与主板是否存在兼容问题，此时可以另外拿一块显卡插在主板上，如果故障解除，则说明兼容问题存在。当然，用户还可以将该显卡插在另一块主板上，如果也没有故障，则说明这块显卡与原来的主板确实存在兼容问题。对于这种故障，最好的解决办法就是换一块显卡或者主板。

（5）检查显卡硬件本身的故障，一般是显示芯片或显存烧毁，建议用户将显卡拿到别的机器上试一试，若确认是显卡问题，更换后即可解决故障。

2. 显示器花屏，看不清字迹

显示器花屏是一种比较常见的显示故障，大部分显示器花屏的故障都是由显卡本身引起的。

第一种故障：一开机就花屏。

【故障表现】：一台计算机一开机就显示花屏，看不清字迹。

【故障分析】：显示器花屏故障大部分都是由网卡本身造成的，可以先从网卡下手排除故障。

【故障排除】：排除故障从以下几个方向操作。

（1）检查显卡是不是存在散热问题，用手触摸一下显存芯片的温度，看看显卡的风扇是否停转。如果散热的确有问题的话，用户可以采用换个风扇或在显存上加装散热片的方法解决故障。

（2）检查一下主板上的 AGP 插槽里是否有灰尘，看看显卡的金手指是否被氧化了，然后可根据具体情况把灰尘清除掉，用橡皮擦把金手指的氧化部分擦亮。

第二种故障：运行程序时花屏。

【故障表现】：一台计算机玩 3D 游戏时显示器花屏，平常操作中并没有此故障。

【故障分析】：从故障现象可以初步判断是显卡驱动与游戏不兼容或者驱动本身的漏洞。

【故障排除】：从官方网站下载最新的显卡驱动程序，卸载显卡驱动后，重新安装新下载的显卡驱动，故障排除。

3. 颜色显示不正常

【故障表现】：一台计算机启动后发现颜色显示不正常，而且饱和度较差。

【故障分析】：上述故障一般是显像管尾部的插座受潮或是受灰尘污染，也可能是其显像管老化造成的。

【故障排除】：对于是受潮或受灰尘污染的情况，如果不很严重，用酒精清洗显像管尾部插座部分即可解决；如果情况严重，就需要更换显像管尾部插座了。

对于显像管老化的情况，只能更换显像管才能彻底解决问题。如果还在保修期内，最好还是先找销售商（或厂商）解决。

4. 屏幕出现异常杂点或花屏

【故障表现】：一台计算机在开机后，屏幕出现异常杂点或图案，甚至花屏。

【故障分析】：此类故障一般是由于显卡质量不好造成的，在显卡工作一段时间后，温度升高，造成显卡的内存、电容等元件工作不稳定而出现问题。

【故障排除】：如果用户的计算机处于超频状态，用户可以将频率修改过来即可；如果是显卡与主板接触不良造成的，用户可以清洁显卡金手指部位或更换显卡的插槽。

5. 显卡驱动程序丢失

【故障表现】：一台计算机重装系统后，运行一段时间后显卡驱动程序自动丢失。重新安装显卡驱动后，故障依然存在。

【故障分析】：此类故障一般是由于显卡质量较差或显卡与主板不兼容，使得显卡温度太高，从而导致系统运行不稳定或出现死机。

【故障排除】：用户首先重装操作系统，如果故障不能排除，则只能更换网卡。

6. 电源功率或设置的影响

现在计算机的主板提供的高级电源管理功能十分多，有节能、睡眠、ONNOW 等，但有些显卡和主板的某些电源功能有时会产生冲突，会导致进入 Windows 后出现花屏的现象。

【故障表现】：一台计算机在调试的过程中，改动了 CMOS 中电源的设置特别是与 VIDEO 相连的设置，结果开机进入操作系统后颜色变成了 256 色，并且还提示要安装新的驱动程序。

【故障分析】：该故障是因为一些基本设置的错误而导致的故障。

【故障排除】：由于当时是改动了 CMOS 电源选项后马上出现了问题，所以把计算机调整为出厂的默认值，即可解决故障。

5.4.5 计算机死机或重启故障分析及解决方案

在 BIOS 自检的过程中，包括有开机、无显示 BIOS 自检和有显示 BIOS 自检的 3 个阶段，因此下面以 Award BIOS 为例，分别对这 3 个阶段进行说明。

1. 开机阶段

【正常情况】：计算机启动的第一步是按下电源开关。计算机接通电源后，首先系统在主板 BIOS 的控制下进行自检和初始化。如果电源工作正常，应该听到电源风扇转动的声音，机箱上的电源指示灯常亮；硬盘和键盘上的“Num Lock”等三个指示灯先亮一下，然后熄灭；显示器也会发出轻微的“唰”声，这比消磁发出的声音会小得多，这是显卡信号送到显示器的反应。

【故障表现】：如果自检无法进行，或键盘的相关指示灯没有按照正常情况闪亮，那么应该着重检查电源、主板和 CPU。因为，此时系统是由主板 BIOS 控制的，在基础自检结束前，是不会检测其他部件的，而且开机自检发出相关的报警声响很有限，显示屏也不会显示有任何相关主机部件启动情况的信息。此时可以从以下几个方面检查。

（1）如果听不到系统自检的“嘟”声，同时看不到电源指示灯亮，以及 CPU 风扇没有转动，应该检查机箱后面的电源接头是否插紧，这时可以将电源接口拔出来重新插入，排除电源线接触不良的原因。当然，电源插座、UPS 保险丝等，这些相关电源的地方也应该仔细检查。

（2）如果电源指示灯亮，但显示屏没有任何信息，没有发出轻微的“唰”声，硬盘和键盘指示灯完全不亮，也没有任何报警声。那么可能是由于曾经在 BIOS 程序中，错误地修改过相关设置，如 CPU 的频率和电压等的设置项目。此外，也很可能是由于 CPU 没有插牢、出现接触不良的现象，或者选用的 CPU 不适合当前的主板使用，或者 CPU 安装不正确，也或者在主板中硬件 CPU 调频设置错误。

这时应该检查 CPU 的型号和频率是否适合当前的主板使用，以及检查 CPU 是否按照正确方法插牢。如果是 BIOS 程序设置错误，可以使用放电方法，将主板上的电池取出，待过了 1 小时左右再将其装回原来的地方，如果主板上具有相关 BIOS 恢复技术，也可使用这些功能。如果是主板的硬件 CPU 调频设置错误，则应该对照主板说明书仔细检查，按照正确的设置，将其调回适当的位置。

（3）若电源指示灯亮，而硬盘和键盘指示灯完全不亮，同时听到连续的报警声，说明主板上的 BIOS 芯片没有装好，或接触不良，或者 BIOS 程序损坏。这时可以关闭电源，将 BIOS 芯片插

牢。否则就可能是由于 BIOS 程序损坏的原因，如受到 CIH 病毒攻击。如果升级过 BIOS 的话，那么也可能是因为在升级 BIOS 时失败所致。不过，在开机自检的故障中，由于 BIOS 芯片没有装好或 BIOS 程序损坏这种情况不常见。

（4）有些机箱制作粗糙，复位键（Reset）按下后弹不起来或内部卡死，会使复位键处于常闭状态，这种情况同样也会导致计算机开机出现故障。这时应该检查机箱的复位键，并将其调好。

2. 无显示 BIOS 自检阶段

【正常情况】：如果硬盘和键盘 Num Lock 等三个指示灯亮一下再灭，系统会发出“嘟”的一声，接着检测显示卡，屏幕左上角出现显卡芯片型号、显示 BIOS 日期等相关信息。

【故障表现】：如果这时自检中断，出现故障，可以从以下几方面检查。

（1）如果计算机发出不间断的长“嘟”声，说明系统没有检测到内存条，或者内存条的芯片损坏。这时可以关闭电源，重新安装内存条，排除接触不良的因素，或者另外更换内存再次开机测试。

（2）计算机发出 1 长 2 短的报警声，说明存在显示器或显卡错误。这时应该关闭电源，检查显卡和显示器插头等部位是否接触良好。如果排除接触不良的原因，则应该更换显卡进行测试。

（3）如果这时自检中断，而且使用了 CPU 非标准外频，以及没有对 AGP/PCI 端口进行锁频设置，那么也可能是由于设置的非标准外频而导致自检中断。这是因为使用了非标准外频，AGP 显卡的工作频率会高于标准的 66MHz，质量较差的显卡就可能通不过。这时可以将 CPU 的外频设置为标准外频，或将在 BIOS 中将 AGP/PCI 端口进行锁频设置，其中 AGP 应该锁在 66MHz 的频率，而 PCI 则应该锁在 33MHz 的频率。

3. 有显示 BIOS 自检阶段

【正常情况】：自检完毕后，就会在显示屏中显示 CPU 型号和工作频率、内存容量、硬盘工作模式，以及所使用的中断号等，高版本的 BIOS 还可以显示 CPU 和机箱内的温度、CPU 和内存的工作电压等数据，如图 5-12 所示。如果 CPU 的工作速度很高，上述 BIOS 信息显示的速度可能很快，这时可以按 Pause 键暂停，查看后再按 Enter 键继续。

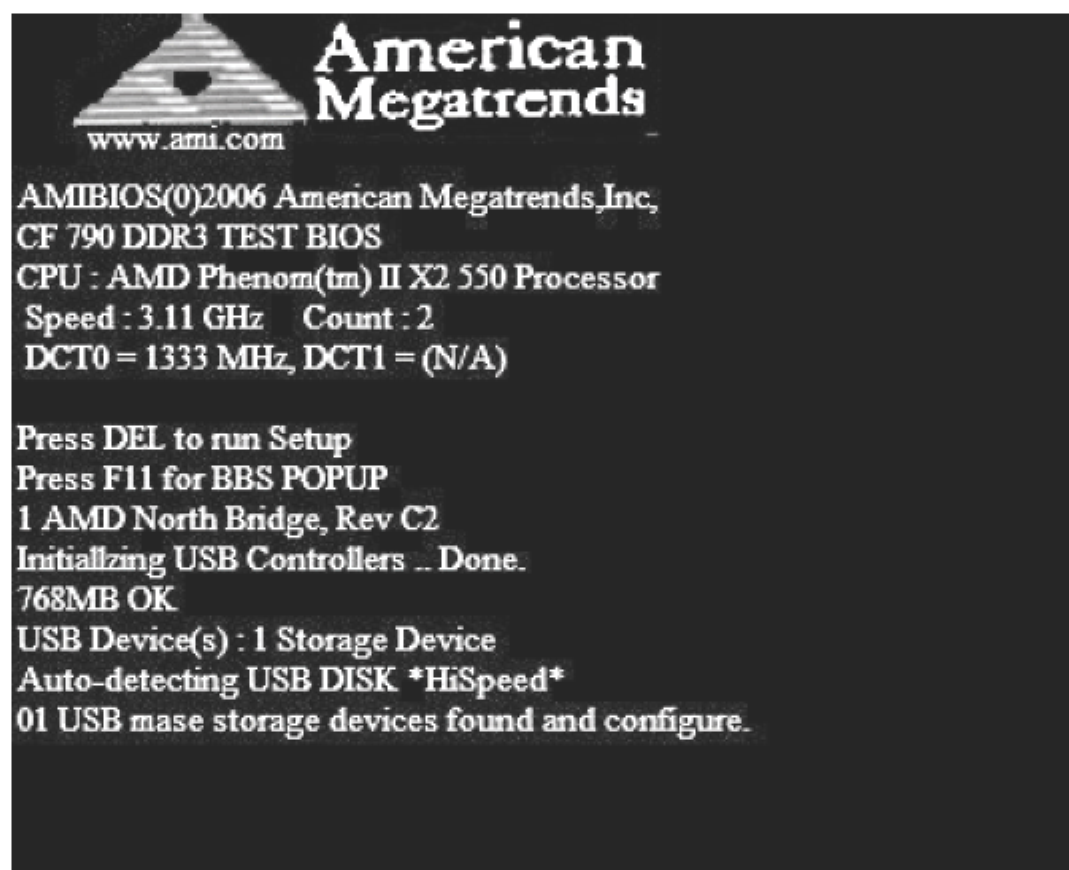


图 5-12　系统开机启动显示信息

【故障表现】：这一阶段可能出现以下常见问题。

（1）检测内存容量的数字，没有检测完就死机。出现这种情况，应该进入 BIOS 的设置程序，检查相关内存的频率、电压和优化项目的设置是否正确。其中，频率和电压设置通常在 BIOS 设置程序的 CPU 频率设置项目中。

```
CPU Internal Core Speed     : 450MHz       PCI/VGA Palette Snoop       : Disabled
                                           Video  ROM BIOS  Shadow     : Enabled
                                           C8000  -  CBFFF  Shadow     : Enabled
Boot Virus Deltection       : Disabled     CC000  -  CFFFF  Shadow     : Enabled
CPU Level 1 Cache           : Enabled      D0000  -  D3FFF  Shadow     : Enabled
CPU Level 2 Cache           : Enabled      D4000  -  D7FFF  Shadow     : Enabled
CPU Level 2 Cache ECC Check : Enabled      D8000  -  DBFFF  Shadow     : Enabled
BIOS Update                 : Enabled      DC000  -  DFFFF  Shadow     : Enabled
Turbo Mode                  : Disabled     Boot Up NumLock Status      : On
Quick Power On Self Test    : Enabled      Typematic Rate Setting      : Disabled
HDD Sequence SCSI/IDE First : IDE          Typematic Rate (Chars/Sec)  : 6
Boot Sequence               : A,C          Typematic Delay (Mesc)      : 250
Boot Up Floppy Seek         : Enabled      Security Option             : Setup
Floppy Disk Access Control  : R/W
IDE HDD Block Mode Sectors  : Disabled
HDD S.M.A.R.T. capability   : Enabled      ESC : Quit        ↑↓→← : Select Item
PS/2 Mouse Function Control : Auto         F1  : Help        PU/PD/+/- : Modify
OS/2 Onboard Memory > 64M   : Disabled     F5  : Old Values  (Shift)F2 : Color
                                           F6  : Load BIOS  Defaults
                                           F7  : Load Setup Defaults
```

图 5-13　BIOS 设置界面

优化设置通常是 BIOS 设置程序【Advanced Chipset Features】选项里面的【DRAM Timing Settings】选项。具体设置可以参考主板的说明书，以及查询相关的资料。

当出现这种情况的时候，应该将相关优化内存的项目设置为不优化或低优化的参数，以及不要对 CPU 和内存进行超频设置，必要时可以选择 BIOS 设置程序的【Load Fail-Safe Defaults】项目，恢复 BIOS 出厂默认值。其次，如果排除以上的原因，那么很可能是由于内存出现兼容或质量方面的问题，这时应该更换内存条进行测试。

（2）显示完 CPU 的频率、内存容量之后，出现【Keyboard error or no keyboard present】的提示。这个提示是指在检测键盘时出现错误，这种情况是由于键盘接口出现接触不良，或者键盘的质量有问题。这时应该关闭计算机，重新安装键盘的接口，如果反复尝试多次都还有这个提示，那么应该更换键盘进行测试。

（3）显示完 CPU 的频率、内存容量之后，出现【Hard disk(s) disagnosis fail】的提示。这个提示是指在检测硬盘时出现错误，这种情况是由于硬盘的数据线或电源线出现接触不良，或者硬盘的质量有问题。这时应该关闭计算机，重新安装硬盘的数据线或电源线，并检查硬盘的数据线和电源线的质量是否可靠。如果排除数据线和电源线的原因，并且反复安装多次都还有这个提示，那么应该更换硬盘进行测试。

（4）显示完 CPU 的频率、内存容量之后，出现【Floppy disk(s) fail】的提示。这个提示是指在检测软驱时出现错误。产生这样的故障原因，可能是在 BIOS 中启用了软驱，但在计算机上却是没有安装软驱。另外，如果连接软驱的数据线或者软驱本身有问题，或者软驱的电源接口和数据线接口接触不良，也会导致这一故障的出现。

5.5　常见软件故障分析及解决方案

在用户使用计算机过程中，由于操作不当、误删除系统文件、病毒木马危害性文件的破坏等

原因，会造成系统出现蓝屏、死机、注册表遭到破坏等操作系统故障。

5.5.1 系统蓝屏故障分析及解决方案

蓝屏是计算机常见的操作系统故障之一，用户在使用计算机过程中会经常遇到。那么计算机蓝屏是由于什么原因引起的呢？计算机蓝屏和硬件关系较大，主要原因有硬件芯片损坏、硬件驱动安装不兼容、硬盘出现坏道（包括物理坏道和逻辑坏道）、CPU 温度过高、多条内存不兼容等。

系统在启动过程中出现如图 5-14 所示的屏幕显示，称做蓝屏。

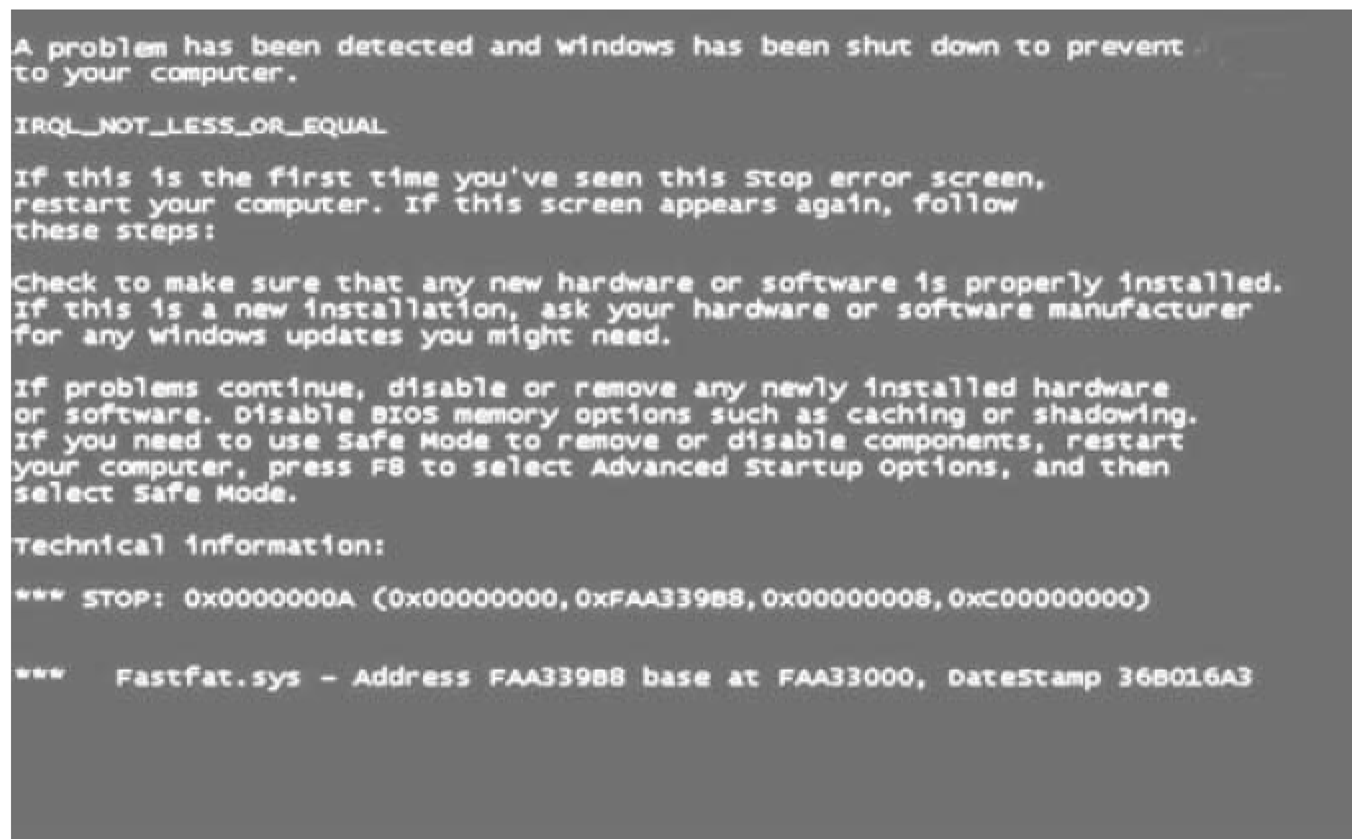


图 5-14　系统蓝屏显示信息



提　示

technical information 以上的信息是蓝屏的通用提示，下面的 0X0000000A 称为蓝屏代码，Fastfat.sys 是引起系统蓝屏的文件名称。

下面介绍几种引起系统开机蓝屏的常见故障原因及解决方法。

1）多条内存条的互不兼容或损坏引起运算错误

这是个最直观的现象，因为这个现象往往在一开机的时候就可以见到。不能启动计算机，画面提示出内存有问题，计算机会询问用户是否要继续。造成这种错误提示的原因，一般是内存的物理损坏或者内存与其他硬件的不兼容所致。这个故障只能通过更换内存来解决问题。

2）系统硬件冲突

这种现象导致蓝屏也比较常见，经常遇到的是声卡或显卡的设置冲突，具体解决的操作步骤如下。

01 开机后，在进入 Windows 系统启动画面之前按 F8 键，显示如图 5-15 所示。

02 使用方向键选择【安全模式】选项。按回车键，进入【安全模式】下的操作系统界面。

03 选择【开始】➢【控制面板】命令，如图 5-16 所示。

04 在弹出的【控制面板】窗口中选择【管理工具】选项，如图 5-17 所示。

05 弹出【管理工具】窗口，选择【计算机管理】选项，如图 5-18 所示。



图 5-15　系统安全模式选项界面



图 5-16　【开始】菜单选项



图 5-17　【控制面板】窗口



图 5-18　【管理工具】窗口

06 弹出【计算机管理】窗口，在【设备管理器】选项页中检查是否存在带有黄色问号或感叹号的设备，若存在可试着先将其删除，并重新启动计算机，如图 5-19 所示。

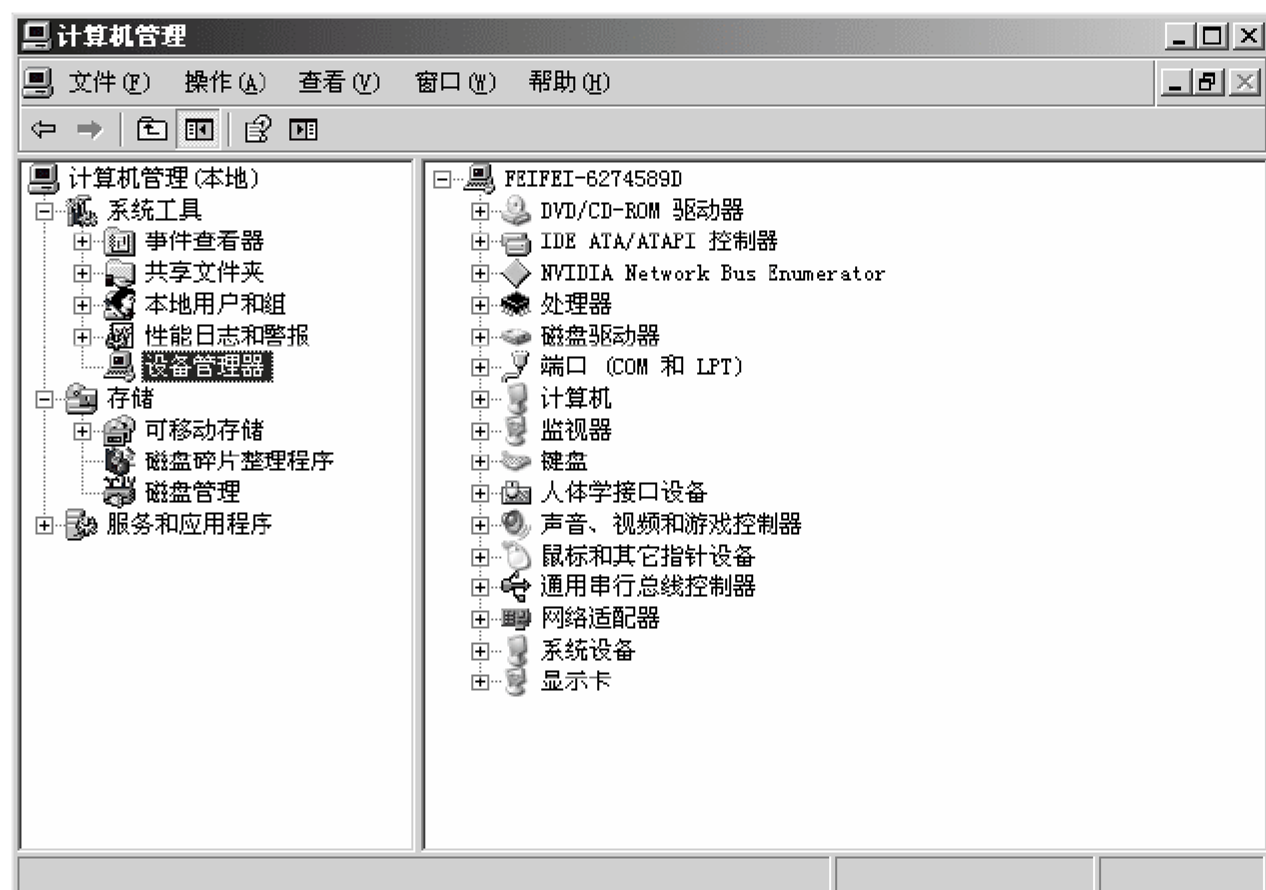


图 5-19　【设备管理器】选项页

带有黄色问号表示该设备的驱动未安装，带有感叹号的设备标示该设备的驱动安装的版本错误。用户可以从设备官方网站下载驱动包安装，或者在随机赠送的驱动盘中找到正确的驱动安装。

如果系统在运行过程中由于某种操作或者没有任何操作而直接出现蓝屏，那么该如何解决呢？下面介绍系统运行过程中蓝屏现象几种常见的原因及解决办法。

1）虚拟内存不足造成系统多任务运算错误

虚拟内存是 Windows 系统所特有的一种解决系统资源不足的方法。一般要求主引导区的硬盘剩余空间是物理内存的 2~3 倍。由于种种原因，造成硬盘空间不足，导致虚拟内存因硬盘空间不足而出现运算错误，所以就会出现蓝屏。要解决这个问题比较简单，尽量不要把硬盘存储空间占满，要经常删除一些系统产生的临时文件，从而可以释放空间；或可以手动配置虚拟内存，把虚拟内存的默认地址，转到其他的逻辑盘下。

虚拟内存具体设置方法如下。

01 右击【桌面】➢【我的电脑】图标，在弹出的快捷菜单中选择【属性】命令，如图 5-20 所示。

02 弹出【系统属性】对话框，选择【高级】选项卡，然后在【性能】选项域中单击【设置】按钮，如图 5-21 所示。

03 弹出【性能选项】对话框，包括【视觉效果】、【高级】和【数据执行保护】3 个选项卡，如图 5-22 所示。

04 选择【高级】选项卡，单击【更改】按钮，如图 5-23 所示。

05 弹出【虚拟内存】对话框，更改系统虚拟内存设置项目，单击【确定】按钮，然后重新启动计算机系统，如图 5-24 所示。



图 5-20 【我的电脑】快捷菜单

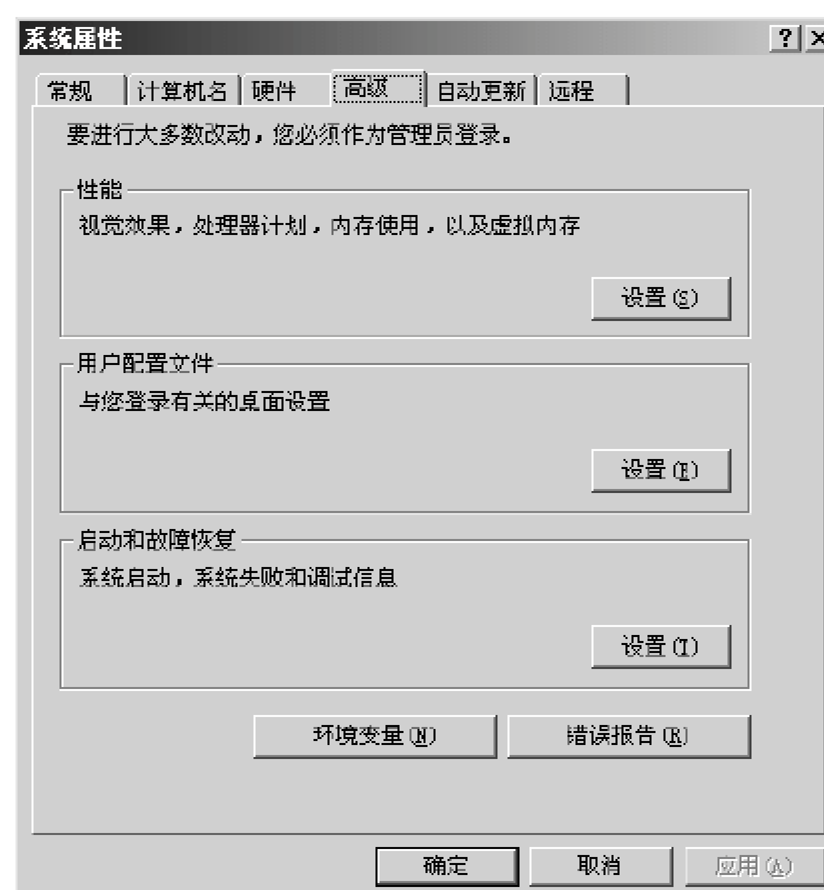


图 5-21 【系统属性】对话框

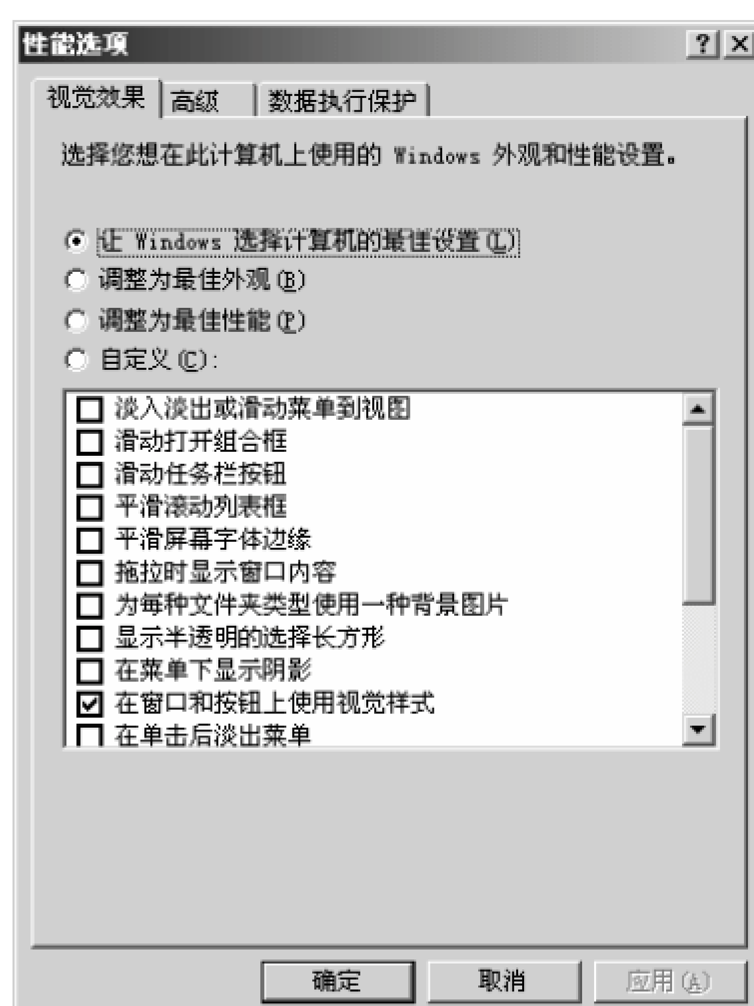


图 5-22 【性能选项】对话框

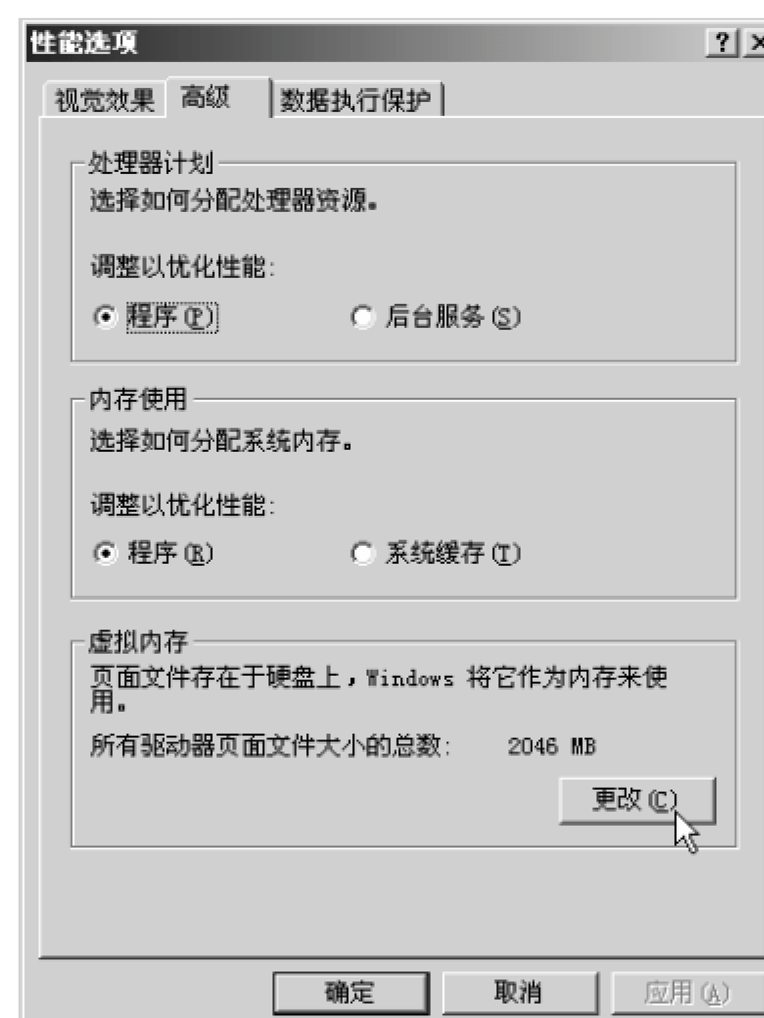


图 5-23 【高级】选项卡

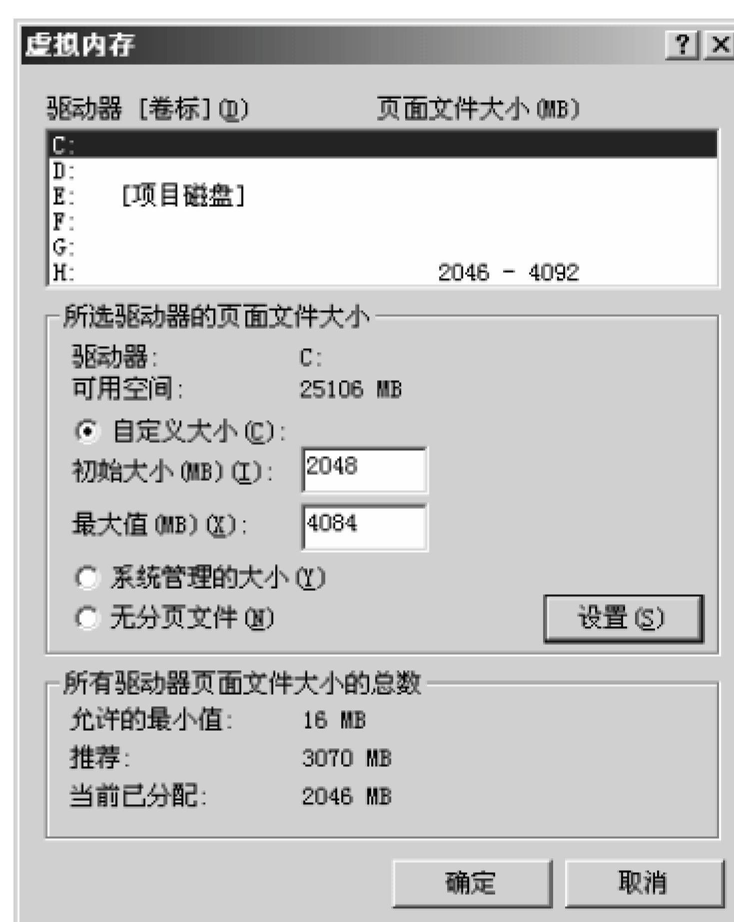


图 5-24 【虚拟内存】对话框

【自定义大小】：根据实际需要在“初始大小”和“最大值”两个文本框中填写虚拟内存在某个盘符的最小值和最大值，单击【设置】按钮，一般最小值是实际内存的 1.5 倍，最大值是实际内存的 3 倍。

【系统管理的大小】：选择此项系统将会根据实际内存的大小自动管理系统在某盘符下的虚拟内存大小。

【无分页文件】：如果计算机的物理内存较大，则无须设置虚拟内存，选择此项，单击【设置】按钮。

2）硬盘剩余空间太小或碎片太多

由于 Windows 运行时需要用硬盘作虚拟内存，这就要求硬盘必须保留一定的自由空间以保证程序的正常运行。一般而言，最低应保证 100MB 以上的空间，否则会因为硬盘剩余空间太小而出现“蓝屏”。另外，硬盘的碎片太多，也容易导致蓝屏的出现。因此，每隔一段时间进行一次碎片整理是必要的。下面详细介绍整理磁盘碎片的具体操作。

01 选择需要整理碎片的磁盘，右击，在弹出的快捷菜单中选择【属性】命令，如图 5-25 所示。

02 弹出【本地磁盘（C: ）属性】对话框，单击【开始整理】按钮，如图 5-26 所示。



图 5-25 本地磁盘属性快捷菜单

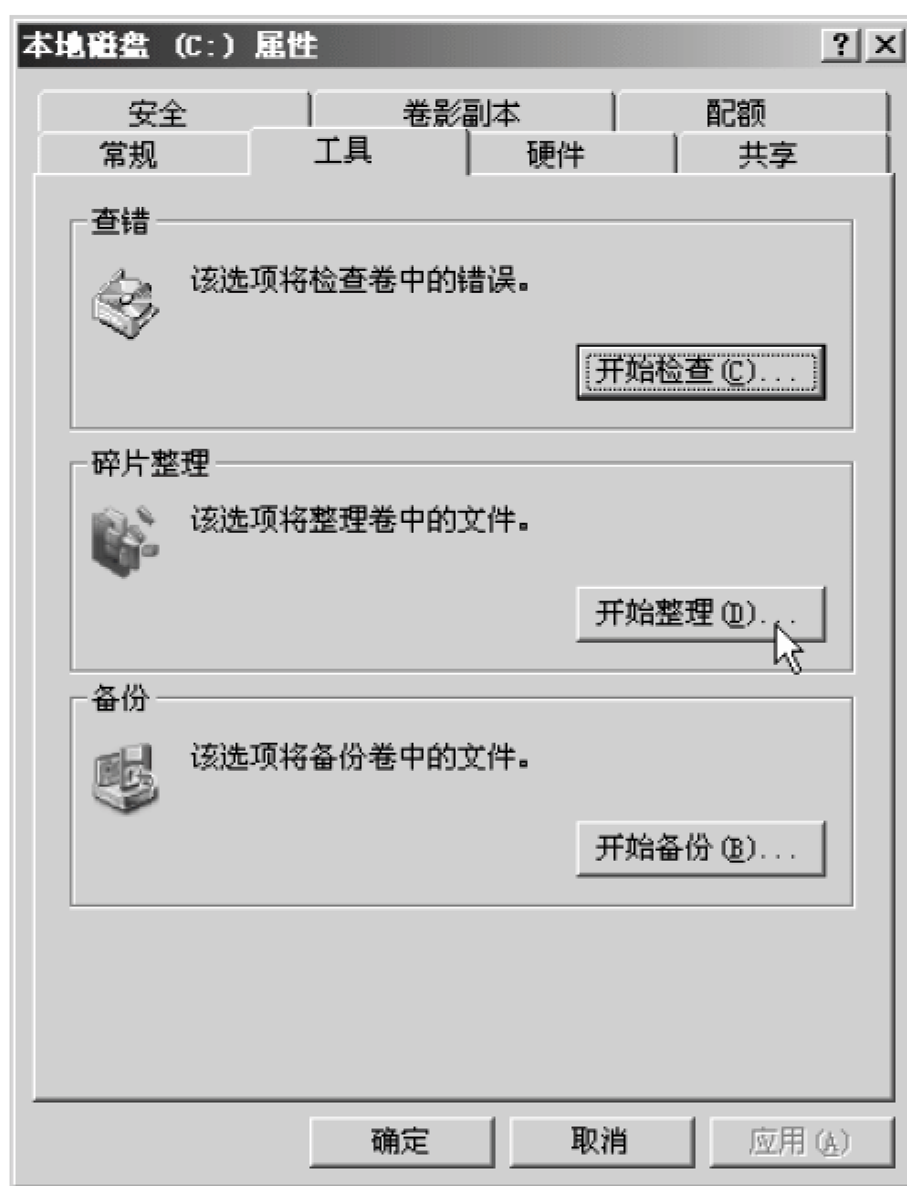


图 5-26 本地磁盘属性对话框

03 弹出【磁盘碎片整理程序】对话框，选择需要磁盘碎片整理的磁盘，单击【碎片整理】按钮，如图 5-27 所示。



图 5-27 【磁盘碎片整理程序】对话框

04 系统先分析磁盘碎片的多少，然后自动整理磁盘碎片，如图 5-28 所示。

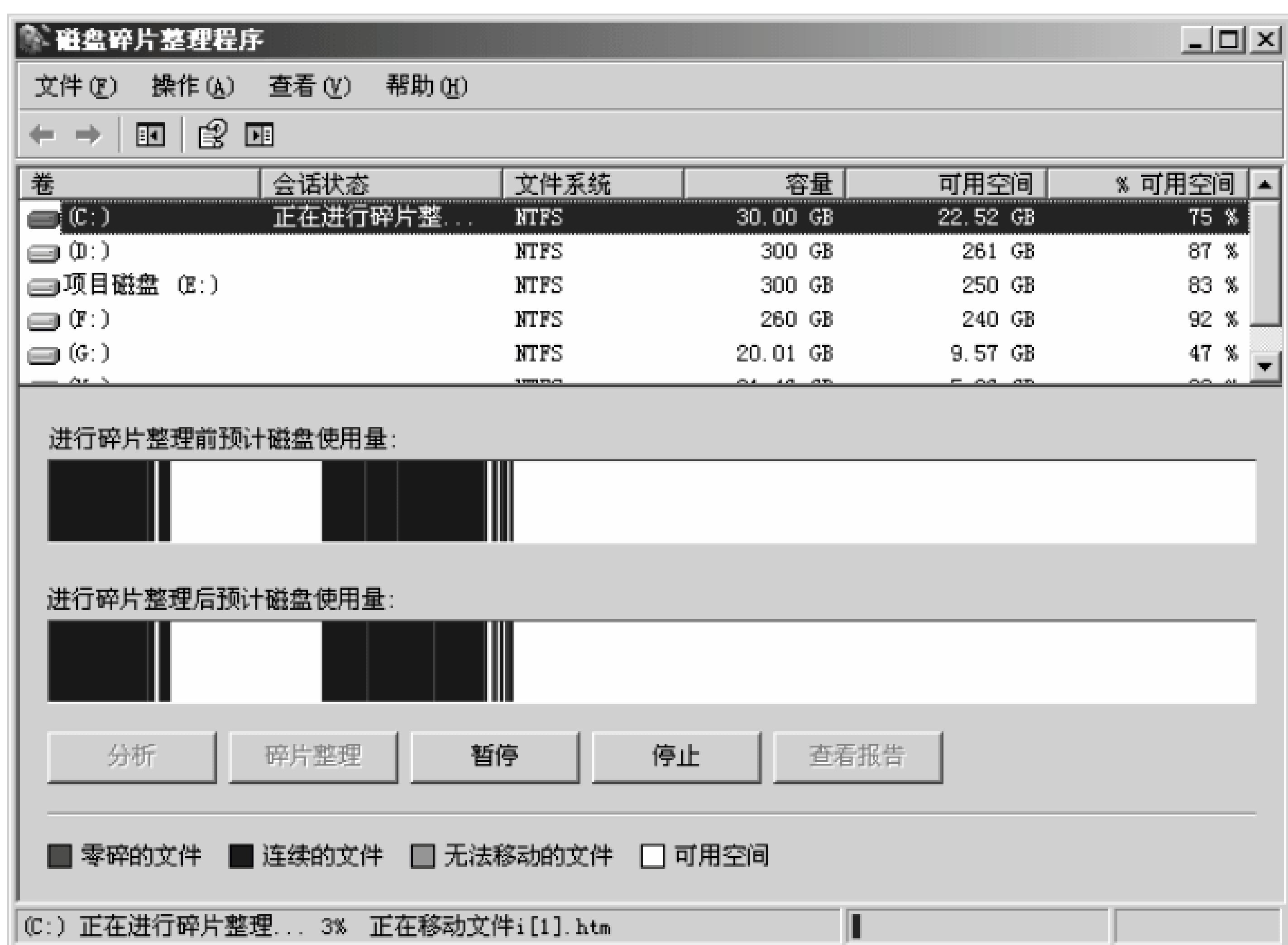


图 5-28 磁盘碎片分析及整理

3）CPU 超频导致运算错误

CPU 超频在一定范围内可以提高计算机的运行速度，就其本身而言是在其原有的基础上完成更高的性能，对 CPU 来说是一种超负荷的工作，CPU 主频变高，运行速度过快，但由于进行了超载运算，造成其内部运算过多，使 CPU 过热，从而导致系统运算错误。

如果是因为超频引起系统蓝屏，在 BIOS 取消 CUP 超频设置，具体的设置根据不同的 BIOS 版本而定。

4）温度过高引起蓝屏

由于机箱散热性问题或者天气本身比较炎热，机箱 CPU 温度过高，计算机硬件系统出于自我保护停止工作。

造成温度过高的原因可能是 CPU 超频，风扇转速不正常，散热功能不好或者 CPU 的硅脂没有涂抹均匀。如果不是超频的原因，最好更换 CPU 风扇或是把硅脂涂抹均匀。

5.5.2　系统死机分析及解决方案

死机，指系统无法从一个系统错误中恢复过来，或系统硬件层面出问题，以致系统长时间无响应，而不得不重启系统的现象。它属于计算机运作的一种正常现象，任何计算机都会出现这种情况，其中蓝屏也是一种常见的死机现象。

1. 系统故障导致死机

Windows 操作系统的系统文件丢失或被破坏时，无法正常进入操作系统，或者“勉强”进入操作系统，但无法正常操作计算机，系统容易死机。

对于一般的操作人员，在使用计算机时，要隐藏受系统保护的文件，以免误删或破坏系统文件。下面详细介绍隐藏受保护的系统文件的方法。

01 打开【我的电脑】窗口，选择【工具】➤【文件夹选项】命令，如图 5-29 所示。



图 5-29　【我的电脑】窗口

02 打开【文件夹选项】对话框。选择【查看】选项卡，选择【隐藏受保护的操作系统文件（推荐）】复选框，单击【确定】按钮，如图 5-30 所示。

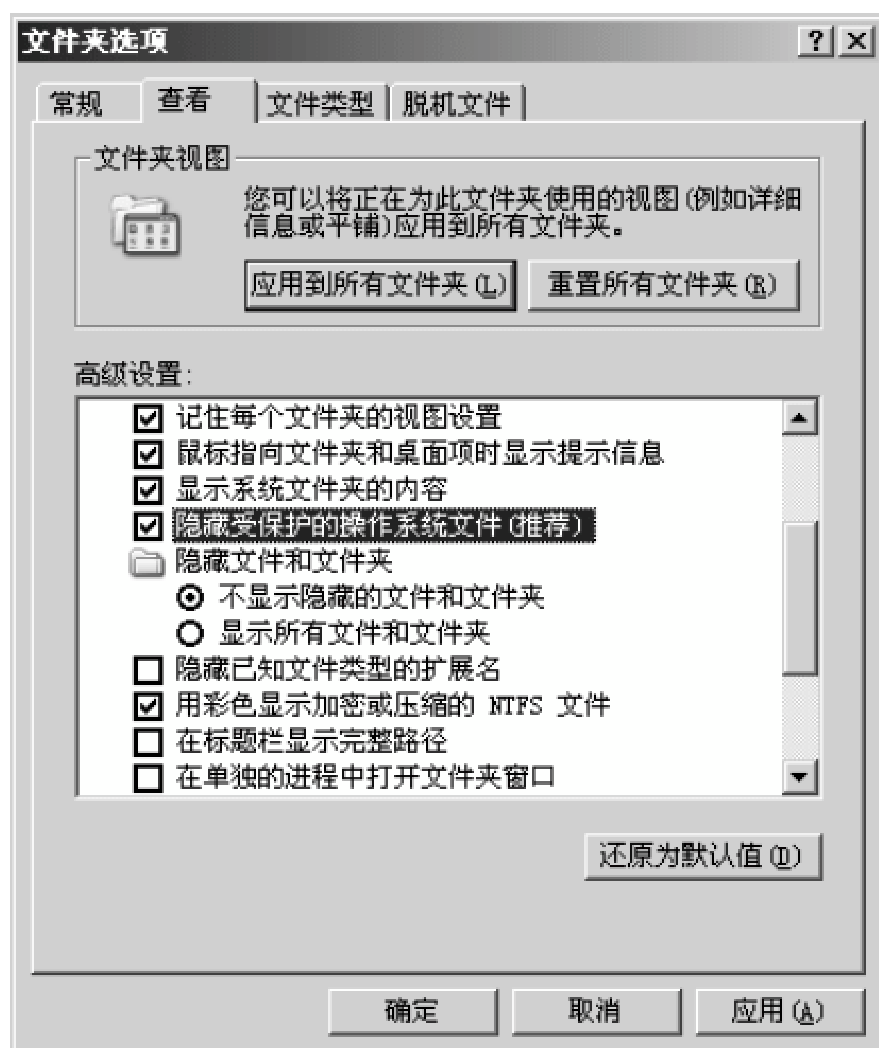


图 5-30　【文件夹选项】对话框

2. 软件故障导致死机

一些用户对计算机的工作原理不是十分了解，出于保证计算机的稳定工作，甚至会在一台计算机装上多个杀毒软件或多个防火墙软件，造成多个软件对系统的同一资源调用或者是因为系统资源耗尽而死机。当计算机出现死机时，可以通过查看开机随机启动项进行排查原因。因为许多应用程序为了用户方便都会在安装完以后，自动添加到 Windows 启动时随机启动项中。下面介绍详细操作步骤。

01 选择【开始】➤【运行】命令，如图 5-31 所示。

02 弹出【运行】对话框，在【打开】输入框中输入“msconfig”，单击【确定】按钮，如图 5-32 所示。



图 5-31 【开始】菜单

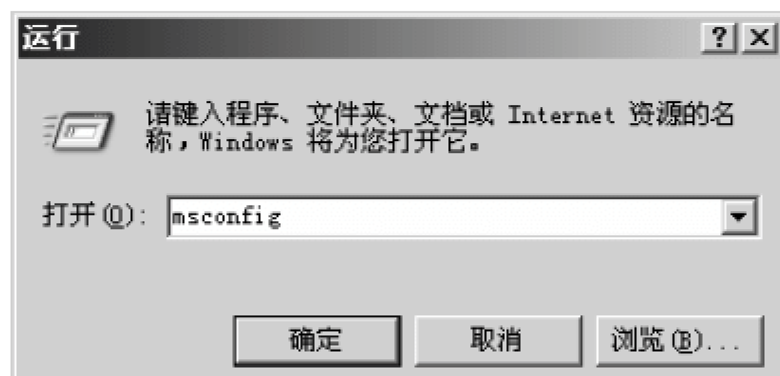


图 5-32 【运行】对话框

03 弹出【系统配置实用程序】对话框。选择【启动】选项卡。启动组中的加载选项全部禁用，然后逐一加载，观察系统在加载哪个程序时出现死机现象，就能查出具体死机的原因了，如图 5-33 所示。



图 5-33 【系统配置实用程序】对话框

5.5.3 注册表常见故障分析及解决方案

注册表在使用中经常会出现故障，下面对常见故障进行介绍。

1. 【我的文档】无法打开，提示【我的文档】被禁用

此故障可能是计算机感染病毒后，被更改了系统注册数值表引起的。打开注册表 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 子键，在右边窗口中将 NosMMyDocs 键值改为 0，可解决此问题，具体操作步骤如下。

01 选择【开始】➢【运行】命令，在弹出的【运行】对话框中输入“regedit”，单击【确定】按钮，打开【注册表编辑器】窗口，如图 5-34 所示。

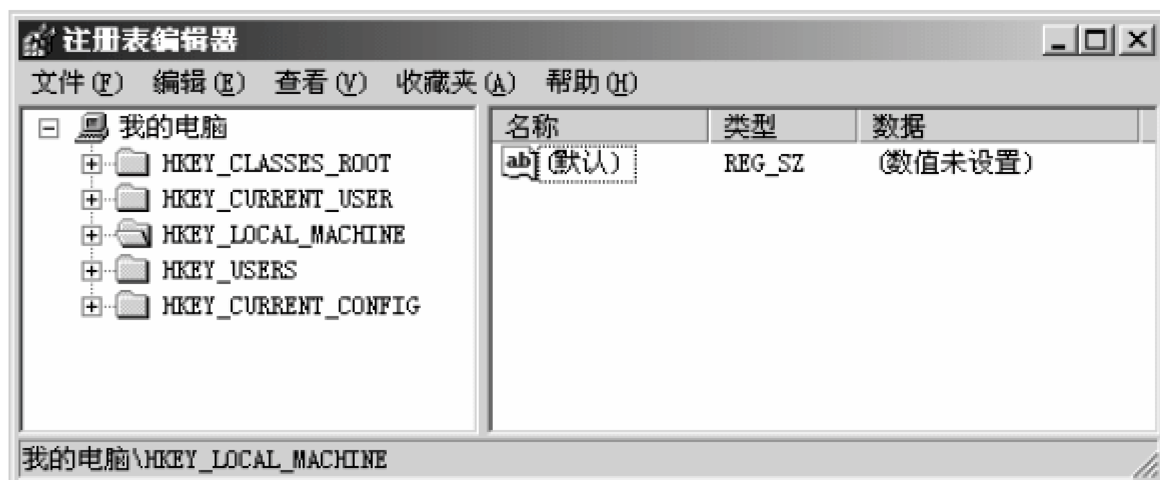


图 5-34 【注册表编辑器】窗口

02 选择【HKEY_CURRENT_USER】➢【Software】➢【Microsoft】➢【Windows】➢【Current Version】➢【Policies】➢【Explorer】选项，如图 5-35 所示。

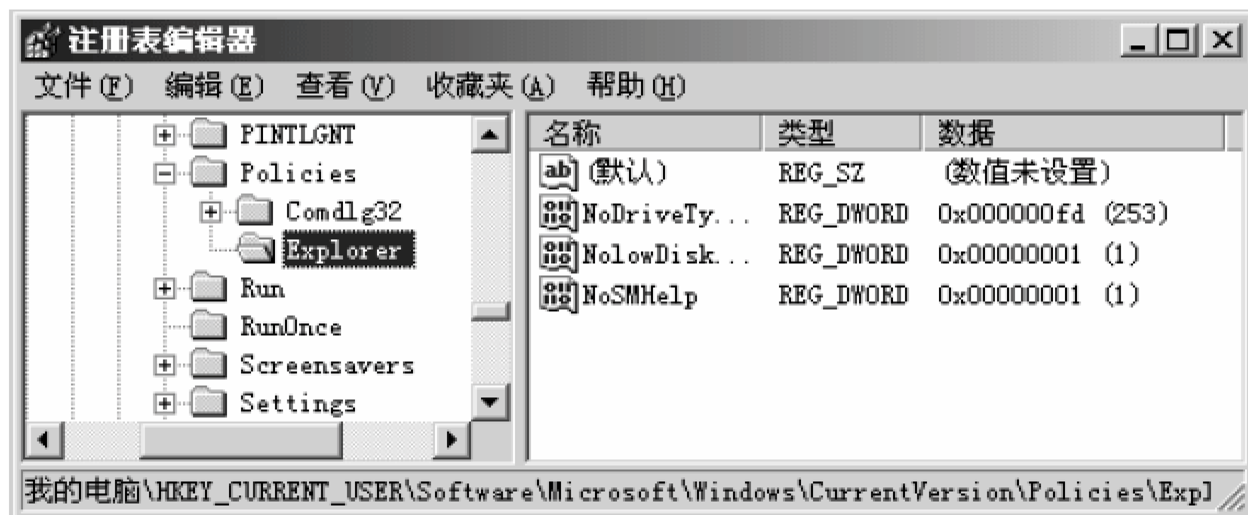


图 5-35 【Explorer】选项页

03 在右侧窗口空白处右击，在弹出的快捷菜单中选择【DWORD 值】菜单命令，如图 5-36 所示。

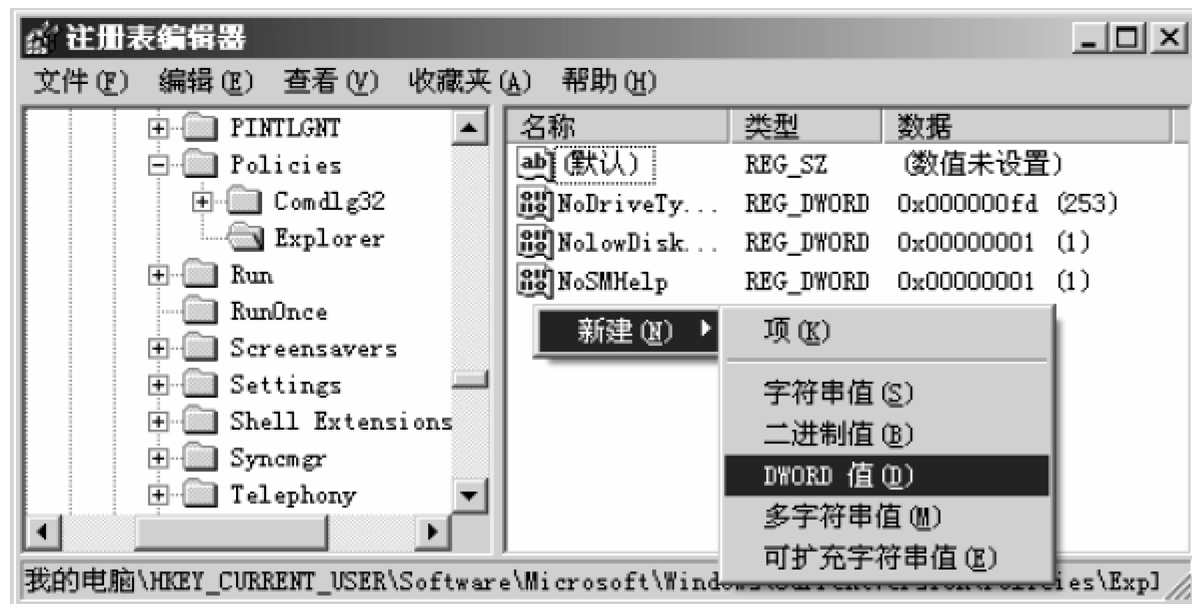


图 5-36 新建【DWORD 值】

04 将新建的子项重命名为【NosMMyDocs】，如图 5-37 所示。

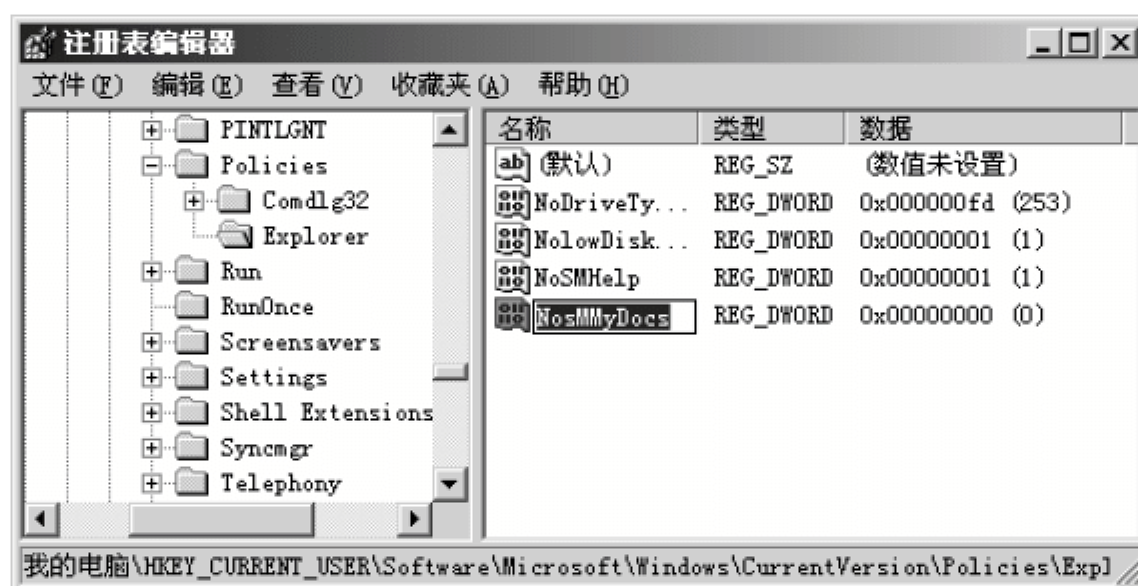


图 5-37　新建名为【NosMMyDocs】的子项

05 右击【NosMMyDocs】选项，在弹出的快捷菜单中选择【修改】命令。弹出【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“0”，单击【确定】按钮，如图 5-38 所示。



图 5-38　【编辑 DWORD 值】对话框

2. 单击鼠标右键无法弹出快捷菜单

遇到此故障一般先检查硬件，鼠标是否损坏，再检查软件，注册表是否设置错误。鼠标故障不再介绍，针对注册表故障，解决方法如下。

在【注册表编辑器】中，选择【HKEY_CURRENT_USER】➢【Software】➢【Microsoft】➢【Windows】➢【CurrentVersion】➢【Policies】➢【Explorer】选项，在右边窗口中将【NoViewContextMenu】键值改为“0”，完成故障修复。具体操作方法与上一故障相似，这里不再详细介绍。

3. 用卸载程序无法将软件卸载

当用户卸载软件的时候会出现软件无法卸载的现象，此故障可能是计算机感染病毒或软件卸载模块被损坏引起的，具体的解决办法如下。

01 用杀毒软件查杀病毒。

02 选择【HKEY_CURRENT_USER】➢【Software】➢【Microsoft】➢【Windows】➢【CurrentVersion】➢【Uninstall】选项，找到该软件的注册项并将其删除，重启计算机生效。

4. 注册表不可用

此故障可能是计算机感染了恶意病毒引起的，需要在【本地组策略编辑器】中配置【阻止访问注册表编辑工具】，具体操作步骤如下。

01 选择【开始】➤【运行】命令，在【运行】对话框中输入 gpedit.msc 命令，如图 5-39 所示。

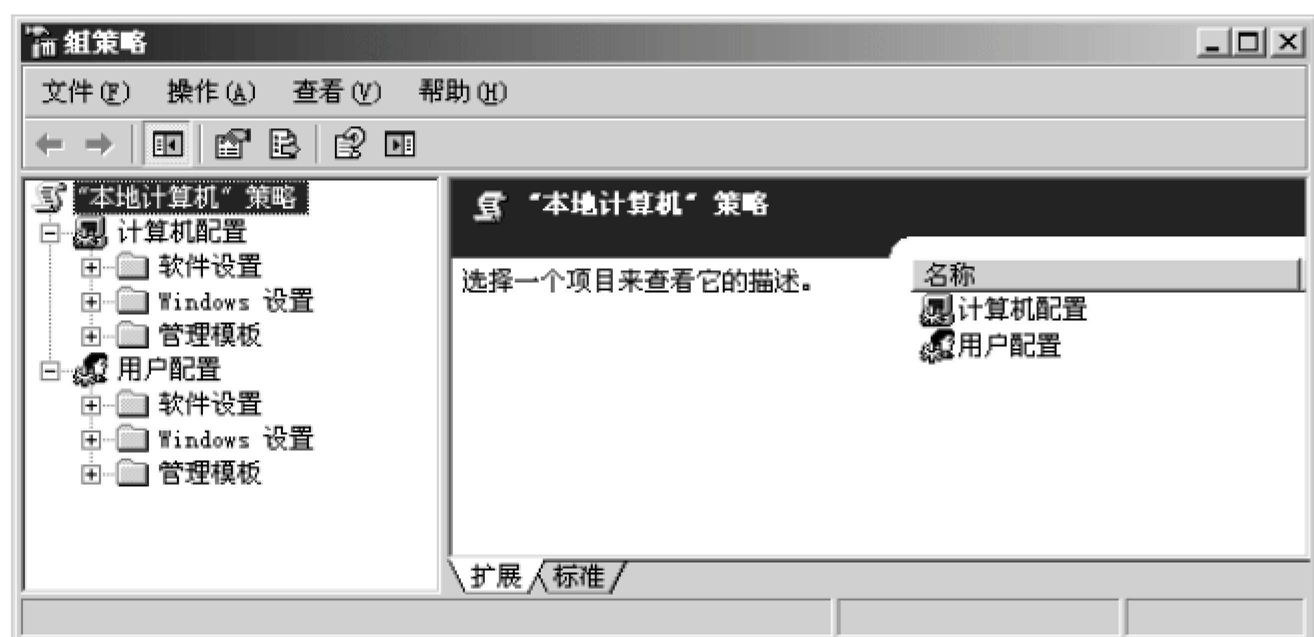


图 5-39　【组策略】窗口

02 选择【用户配置】➤【管理模板】➤【系统】选项，双击右侧窗口中的【阻止访问注册表编辑工具】选项，如图 5-40 所示。



图 5-40　【系统】选项页

03 打开【阻止访问注册表编辑工具 属性】对话框，选中【已禁用】单选按钮，单击【确定】按钮，如图 5-41 所示。

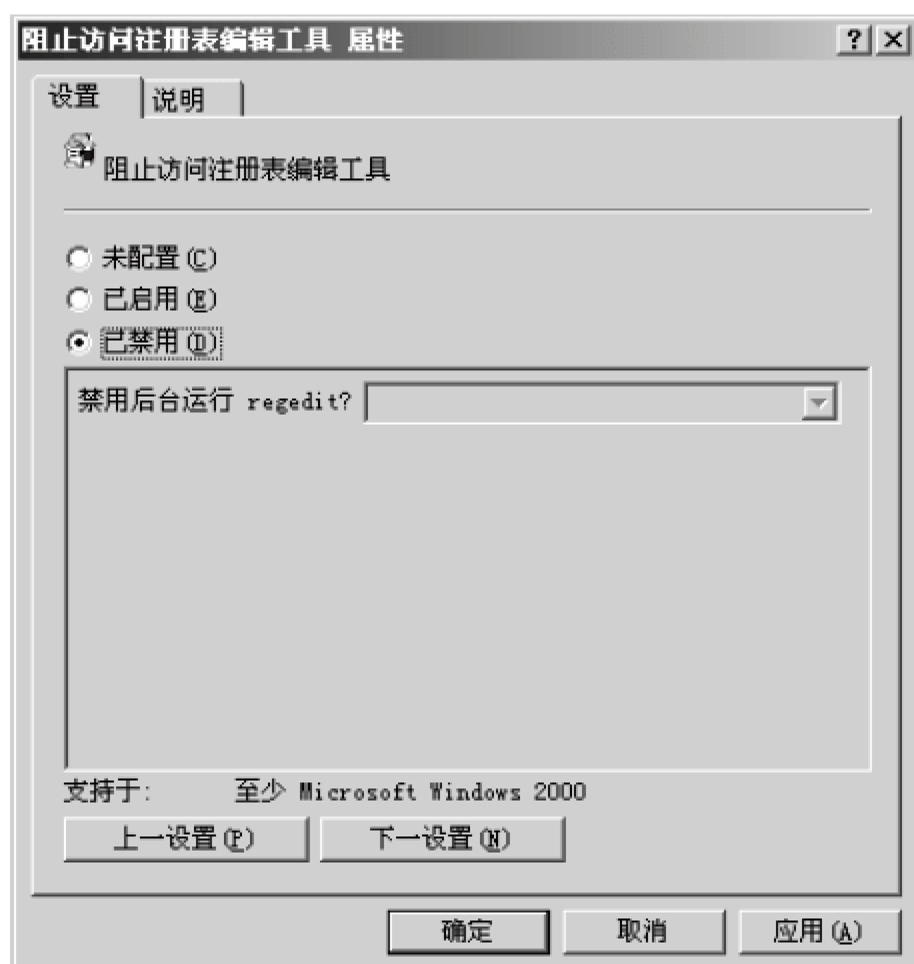


图 5-41　【阻止访问注册表编辑工具　属性】对话框

5.5.4　键盘无法输入故障的解决方案

【故障表现】：一台正常运行的计算机，在玩游戏时切换了一下界面，然后键盘就不能输入了，重启计算机后，故障依然存在。

【故障分析】：首先看一下键盘指示灯是否还亮，如果不亮，可以将键盘插头重新插拔一次，重新操作后，故障依然存在。然后新换了一个正常工作的键盘，还是不能解决问题。这时可以初步判定是系统的问题。

【故障排除】：升级病毒库，然后全盘杀毒，发现一个名为“TrojanSpy.KeyLogger.uh”，此病毒是键盘终结者病毒的变种，经过杀毒后，重新启动计算机后，故障消失。

5.5.5　BIOS 密码忘记解决方案

如果用户不知道原来的密码，可以将密码清除。

BIOS 密码清除的具体操作步骤如下。

01 在开机时按 F2 键，进入 BIOS 设置界面，如图 5-42 所示。

02 按→键，将光标定位在 Security 选项卡下，则光标自动定位在【Set Supervisor Password】选项上，如图 5-43 所示。

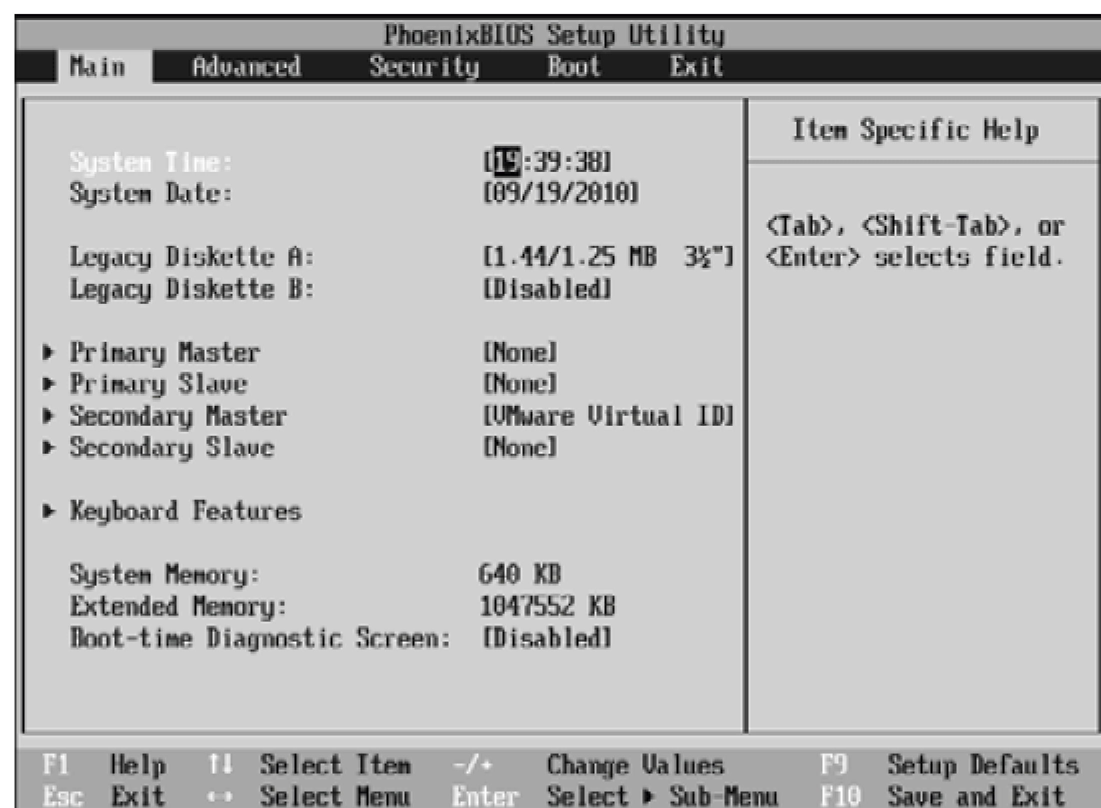


图 5-42　BIOS 设置界面

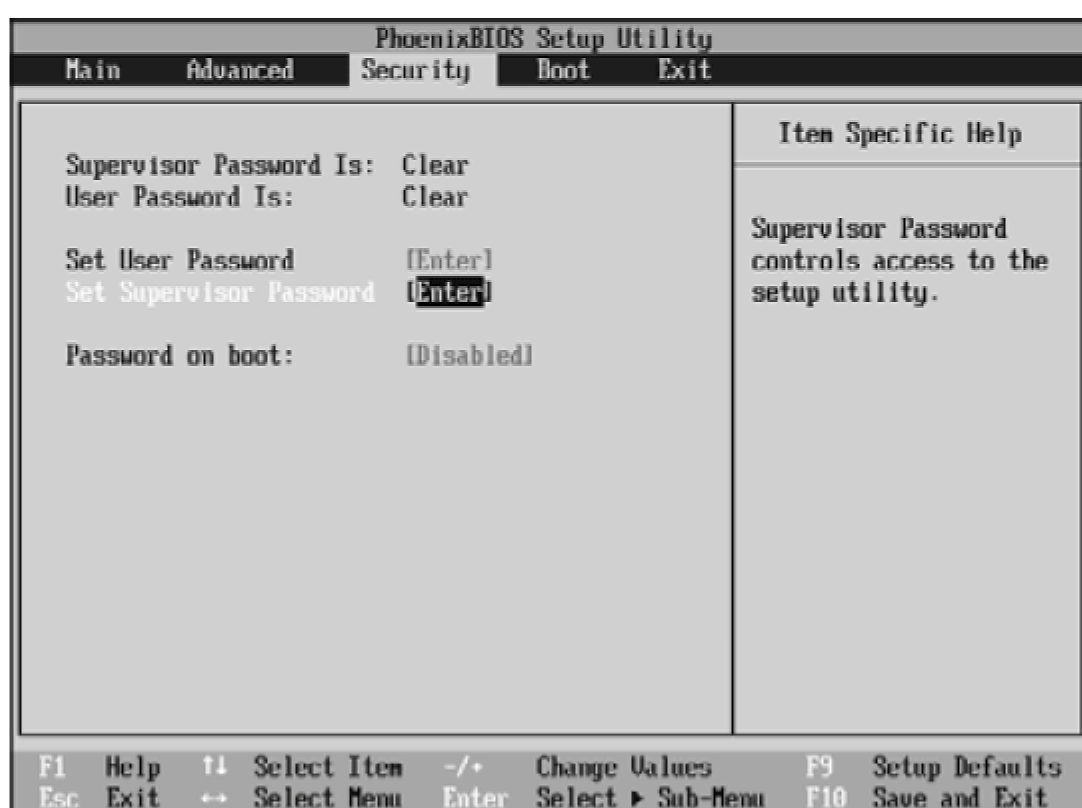
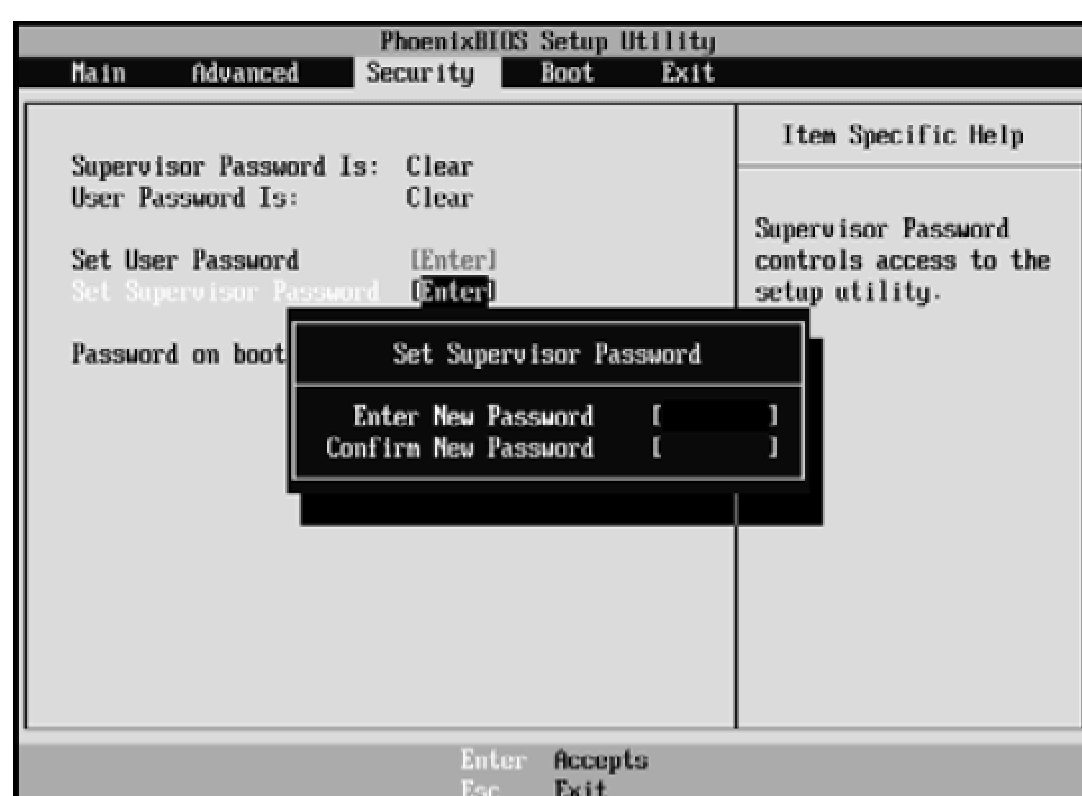


图 5-43　【Security】选项卡

03 按 Enter 键，即可弹出 Set Supervisor Password 提示框，在 Enter New Password 文本框中输入设置的新密码，如图 5-44 所示。

04 按 Enter 键，将光标定位在 Confirm New Password 文本框中再次输入密码，如图 5-45 所示。



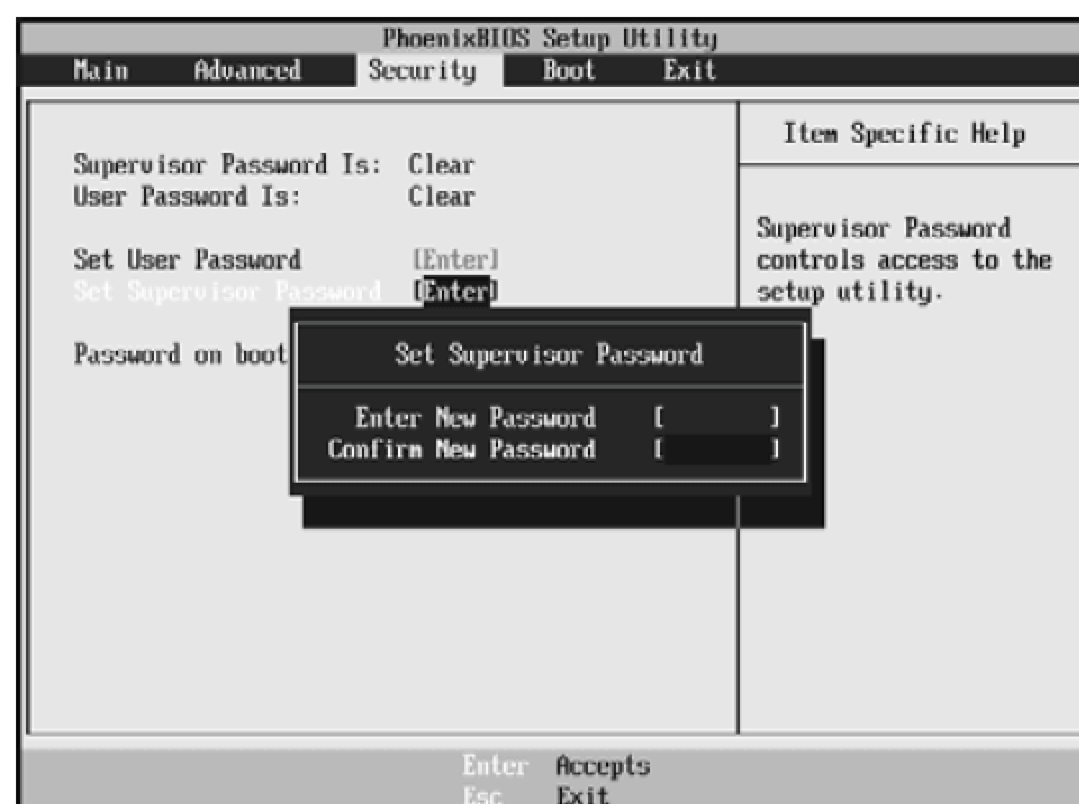


图 5-44　【Set Supervisor Password】提示框　　　图 5-45　确认密码

05 输入完毕后，按 Enter 键，即可弹出【Setup Notice】提示框，选择 Continue 选项，并按 Enter 键确认，即可保存设置的密码，如图 5-46 所示。

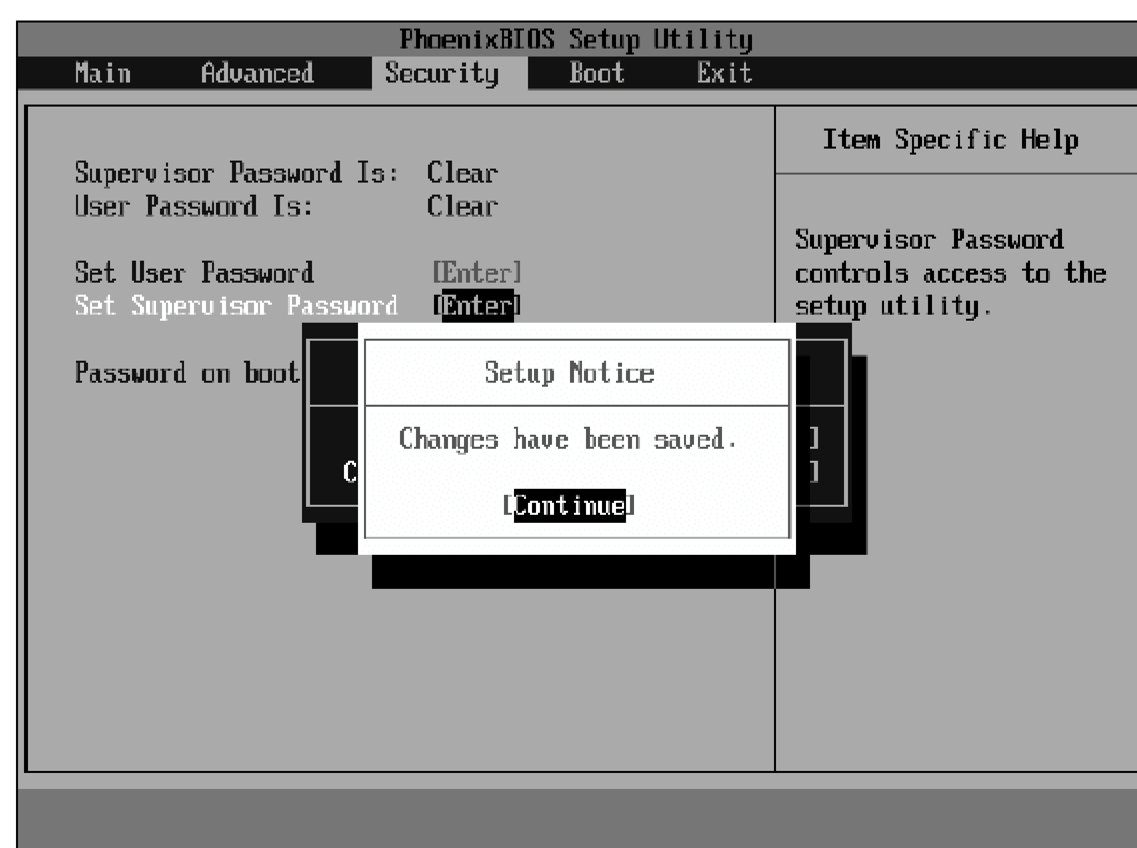


图 5-46　Setup Notice 提示框

为了保护计算机的资源和安全，可以为其加上开机密码。但是不小心将密码忘记，就会致使计算机不能进入 BIOS 设置，或者不能启动计算机。

建议采用如下方法进行处理：

（1）可先试一下通用口令，如 AMIBIOS 的通用口令是“AMI”，AWARDBIOS 的通用口令比较多，可能有“AWARD”，“H996”，“Syzx”，“WANTGIRL”，“AwardSW”等，但通用口令不是万能的。

（2）如果计算机能启动，但不能进入 CMOS 设置，可以在启动 DOS 后，执行下面程序段来完成对所有 CMOS 的清除。

C：\debug

-O180　20

-O181　20

（3）打开机箱后，在主板上找到清除 CMOS 内容的跳线，将其短接三五秒后再开机，CMOS 内容会恢复为出厂时的设置。

5.6　项目实战：BIOS 设置全攻略

所谓 BIOS，实际上就是微机的基本输入输出系统(Basic Input Output System)，其内容集成在微机主板上的一个 ROM 芯片上，主要保存着有关微机系统最重要的基本输入输出程序，系统信息设置，开机上电自检程序和系统启动自举程序等。

5.6.1　BIOS 介绍与常用设置

BIOS 芯片是主板上一块长方形或正方形芯片，如图 5-47 和图 5-48 所示。

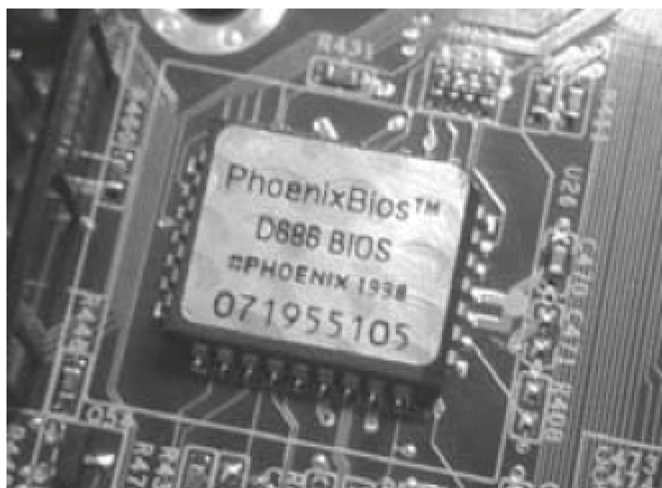


图 5-47　长方形 BIOS 芯片

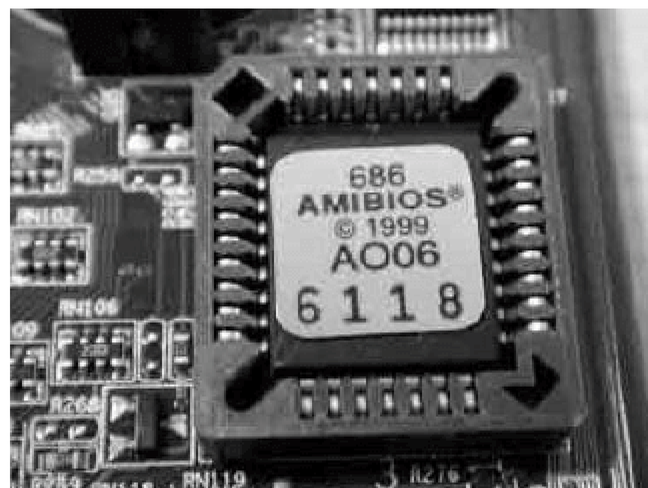


图 5-48　正方形 BIOS 芯片

在 BIOS 中主要存放了如下内容。

（1）自诊断程序，通过读取 CMOS RAM 中的内容识别硬件配置，并进行自检和初始化。

（2）CMOS 设置程序，引导过程中用特殊热键启动，进行设置后存入 CMOS RAM 中。

（3）系统自举装载程序，在自检成功后将磁盘相对 0 道 0 扇区上的引导程序装入内存，让其运行以装入 DOS 系统。



提　示

在 MS-DOS 操作系统中，即使操作系统在运行，BIOS 也仍提供计算机运行所需要的各种信息，但是在 Windows 操作系统中，启动 Windows 操作系统后，BIOS 一般不会再被利用，因为 Windows 操作系统代替 BIOS 完成了 BIOS 运算和驱动器运算的操作。

从功能上看，BIOS 的作用主要有如下几个方面。

1．加电自检及初始化

用于计算机刚接通电源时对硬件部分的检测，功能是检查计算机是否良好，如图 5-39 所示。通常完整的自检包括对 CPU、基本内存、扩展内存、ROM、主板、CMOS 存储器、串并口、显卡、软硬盘子系统及键盘等进行测试，一旦在自检中发现问题，系统将给出提示信息或鸣笛警告。对于严重故障（致命性故障）则停机，不给出任何提示或信号；对于非严重故障则给出提示或声音报警信号，等待用户处理。

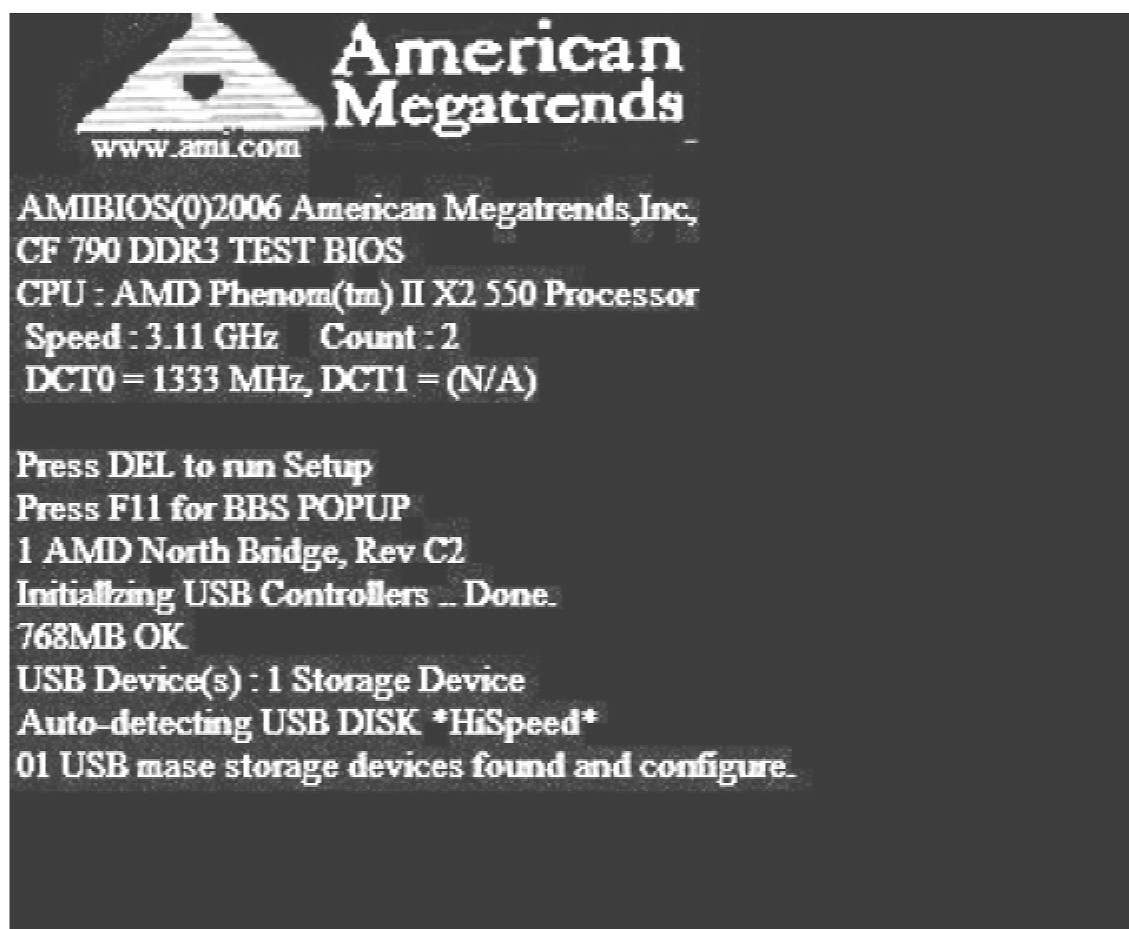


图 5-49　系统启动硬件检测

初始化包括创建中断向量、设置寄存器、对一些外部设备进行初始化和检测等，其中很重要的一部分是 BIOS 设置，主要是对硬件设置的一些参数，当计算机启动时会读取这些参数，并和实际硬件设置进行比较，如果不符合，会影响系统的启动。

2. 引导程序

在对计算机进行加点自检和初始化后，下面需要利用 BIOS 引导 DOS 或其他操作系统。这时，BIOS 先从软盘或硬盘的开始扇区读取引导记录，若没有找到，则会在显示器上显示没有引导设备。若找到引导记录会把计算机的控制权转给引导记录，由引导记录把操作系统装入计算机，在计算机启动成功后，BIOS 的这部分任务就完成了。

3. 程序服务处理

程序服务处理指令主要是为应用程序和操作系统服务，为了完成这些服务，BIOS 必须直接与计算机的 I/O 设备打交道，通过端口发出命令，向各种外部设备传送数据以及从它们那儿接收数据，使程序能够脱离具体的硬件操作。

4. 硬件中断处理

在开机时，BIOS 会通过自检程序对计算机硬件进行检测，同时会告诉 CPU 各硬件设备的中断号。例如，视频服务，中断号为 10H；屏幕打印，中断号为 05H；磁盘及串行口服务，中断号为 14H。当用户发出使用某个设备的指令后，CPU 就根据中断号使用相应的硬件完成工作，再根据中断号跳回原来的工作。

进入 Award BIOS 以后，即可看到其主界面，如图 5-50 所示。Award BIOS 中每一项设置都不相同，也都有着不同的含义。下面对其常见的选项的含义进行详细的介绍。

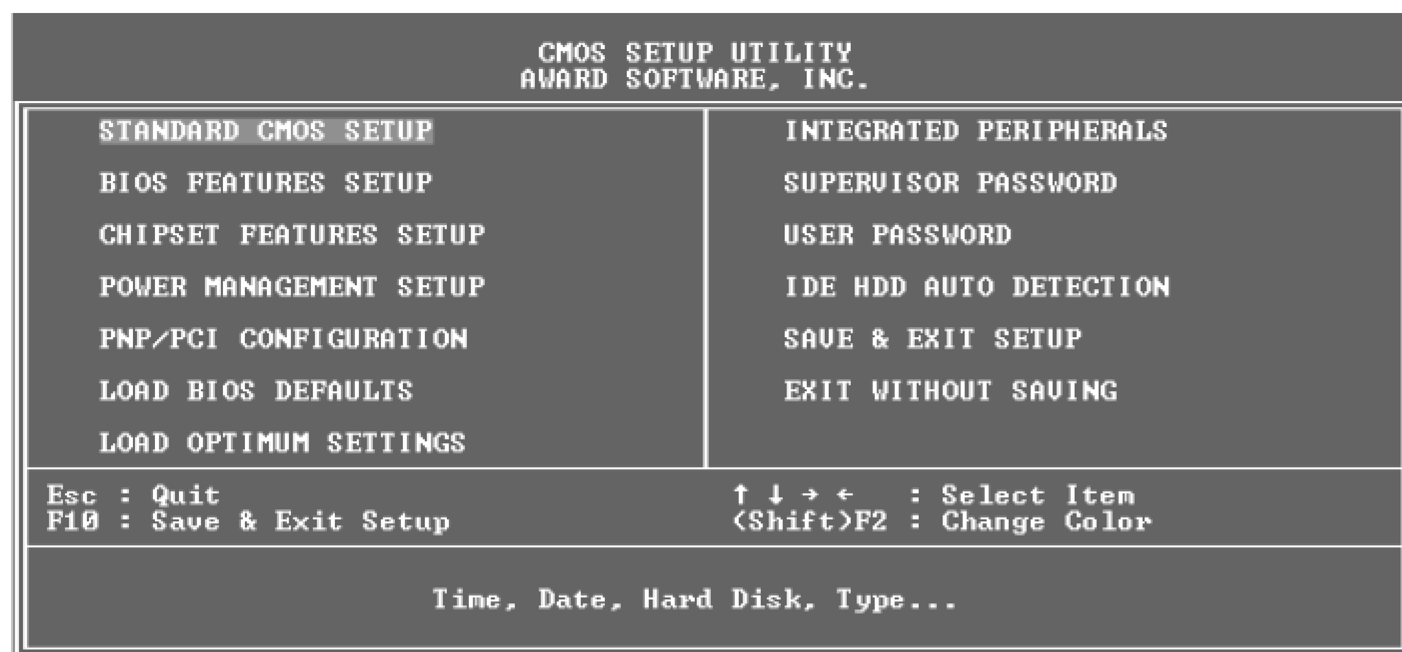


图 5-50　Award BIOS 界面

在 Award BIOS 的主菜单中，主要有如下几个菜单项。

1）STANDARD CMOS SETUP（标准 CMOS 设置）

用于设定本计算机的日期、时间、软硬盘规格、工作类型以及显示器类型等。图 5-51 所示为标准 CMOS 设置界面。

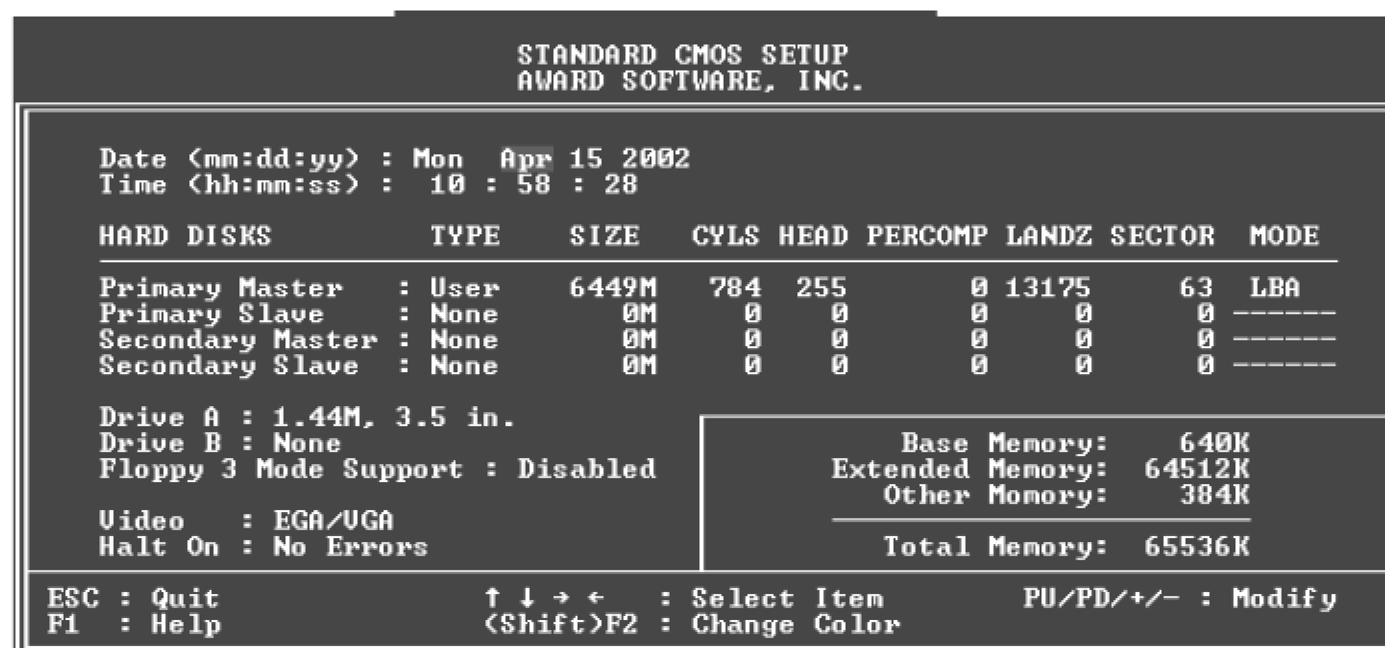


图 5-51　标准 CMOS 设置界面

2）BIOS FEATURES SETUP（BIOS 特性设置）

用于设置定本计算机 BIOS 的特殊功能，例如病毒警告、开机磁盘优先程序等。图 5-52 所示为 BIOS 特性设置界面。

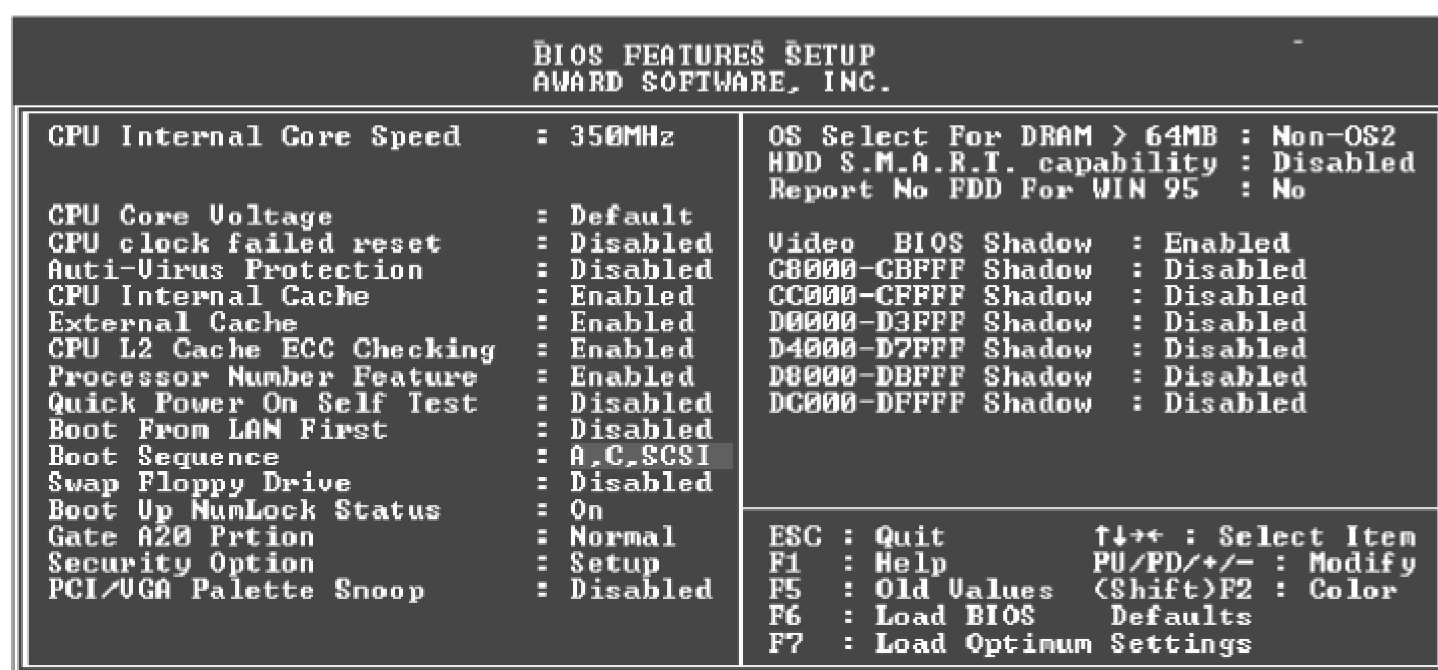


图 5-52　BIOS 特性设置界面

3）CHIPSET FEATURES SETUP（芯片组工作特性设置）

用于设置本计算机 CPU 工作的相关参数。图 5-53 所示为芯片组工作特性设置界面。

```
CHIPSET FEATURES SETUP
AWARD SOFTWARE, INC.

Auto Configuration           : Enabled    | Auto Detect DIMM/PCI Clk : Enabled
EDO DRAM Speed Selection     : 60ns       | Spread Spectrum          : Disabled
EDO CASx# MA Wait State      : 2          |
EDO RASx# Wait State         : 2          | Current CPU Temperature  : 44°C/111°F
SDRAM RAS-to-CAS Delay       : 3          | Current System Temp.     : 40°C/105°F
SDRAM RAS Precharge Time     : 3          | Current CPU FAN Speed    : 4137 RPM
SDRAM CAS latency Time       : 3          | Current CAS FAN Speed    :    0 RPM
SDRAM Precharge Control      : Disabled   | Analog(V)                :  5.16 V
DRAM Data Integrity Mode     : Non-ECC    | I/O   (V)                :  3.40 V
System BIOS Cacheable        : Disabled   | +12   (V)                : 12.10 V
Video  BIOS Cacheable        : Disabled   | CPU   (V)                :  2.05 V
Video RAM Cacheable          : Disabled   |
8 Bit I/O Recovery Time      : 3          |
16 Bit I/O Recovery Time     : 2          |
Memory Hole At 15M-16M       : Disabled   |
Passive Release              : Enabled    | ESC : Quit       ↑↓→← : Select Item
Delayed Transaction          : Disabled   | F1  : Help       PU/PD/+/- : Modify
AGP Aperture Size (MB)       : 64         | F5  : Old Values  (Shift)F2 : Color
On Board Sound               : Enabled    | F6  : Load BIOS   Defaults
On Board Modem               : Enabled    | F7  : Load Optimum Settings
```

图 5-53　芯片组工作特性设置界面

4）POWER MANAGEMENT SETUP（能源管理参数设置）

用于设置本计算机中 CPU、硬盘、显示器等设备的省电功能。图 5-54 所示为能源管理参数设置界面。

```
POWER MANAGEMENT SETUP
AWARD SOFTWARE, INC.

ACPI Suspend Type      : S1(POS)      | ** Reload Global Timer Events **
Power Management       : User Define  | IRQ[3-7,9-15],NMI     : Disabled
PM Control by APM      : Yes          | Primary IDE 0         : Disabled
Video Off Method       : DPMS         | Primary IDE 1         : Disabled
Video Off After        : Standby      | Secondary IDE 0       : Disabled
MODEM Use IRQ          : 3            | Secondary IDE 1       : Disabled
Doze Mode              : Disable      | Floppy Disk           : Disabled
Standby Mode           : Disable      | Serial Port           : Enabled
Suspend Mode           : Disable      | Parallel Port         : Disabled
HDD Power Down         : Disable      |
Throttle Duty Cycle    : 62.5%        |
PCI/VGA Act-Monitor    : Disabled     |
Soft-Off by PWR-BTTN   : Instant-Off  |
Resume by Ring/LAN     : Disabled     |
Wake Up On PCI PME#    : Disabled     |
Resume by Alarm        : Disabled     | ESC : Quit       ↑↓→← : Select Item
                                      | F1  : Help       PU/PD/+/- : Modify
                                      | F5  : Old Values  (Shift)F2 : Color
IRQ 8 Break Suspend    : Disabled     | F6  : Load BIOS   Defaults
                                      | F7  : Load Optimum Settings
```

图 5-54　能源管理参数设置界面

5）PNP/PCI CONFIGURATION（即插即用和 PCI 特性设置）

用于设置本计算机中的即插即用设备和 PCI 设备的有关属性。图 5-55 所示为即插即用和 PCI 特性设置界面。

```
CMOS Setup Utility - Copyright (C) 1984-2002 Award Software
PnP/PCI Configurations

   Reset Configuration Data   [Disabled]    |       Item Help
                                            | Menu Level   ►
   Resources Controlled By    [Auto(ESCD)]  |
 x IRQ Resources               Press Enter  | Default is Disabled.
                                            | Select Enabled to
   PCI/VGA Palette Snoop      [Disabled]    | reset Extended System
                                            | Configuration Data
                                            | ESCD) when you exit
                                            | Setup if you have
                                            | installed a new add-on
                                            | and the system
                                            | reconfiguration has
                                            | caused such a serious
                                            | conflict that the OS
                                            | cannot boot

↑↓→←:Move  Enter:Select  +/-/PU/PD:Value  F10:Save  ESC:Exit  F1:General Help
  F5: Previous Values    F6: Fail-Safe Defaults    F7: Optimized Defaults
```

图 5-55　即插即用和 PCI 特性设置界面

6）LOAD BIOS DEFAULTS（载入 BIOS 预设值）

用于载入本计算机的 BIOS 初始设置值。

7）LOAD OPRIMUM SETTINGS（载入主板 BIOS 出厂设置）

该菜单项是 BIOS 的基本设置，用于确定本计算机的故障范围。

8）INTEGRATED PERIPHERALS（内建整合设备周边设定）

用于设置本计算机集成主板上外部设备的属性。图 5-56 所示为内建整合设备周边设定设置界面。

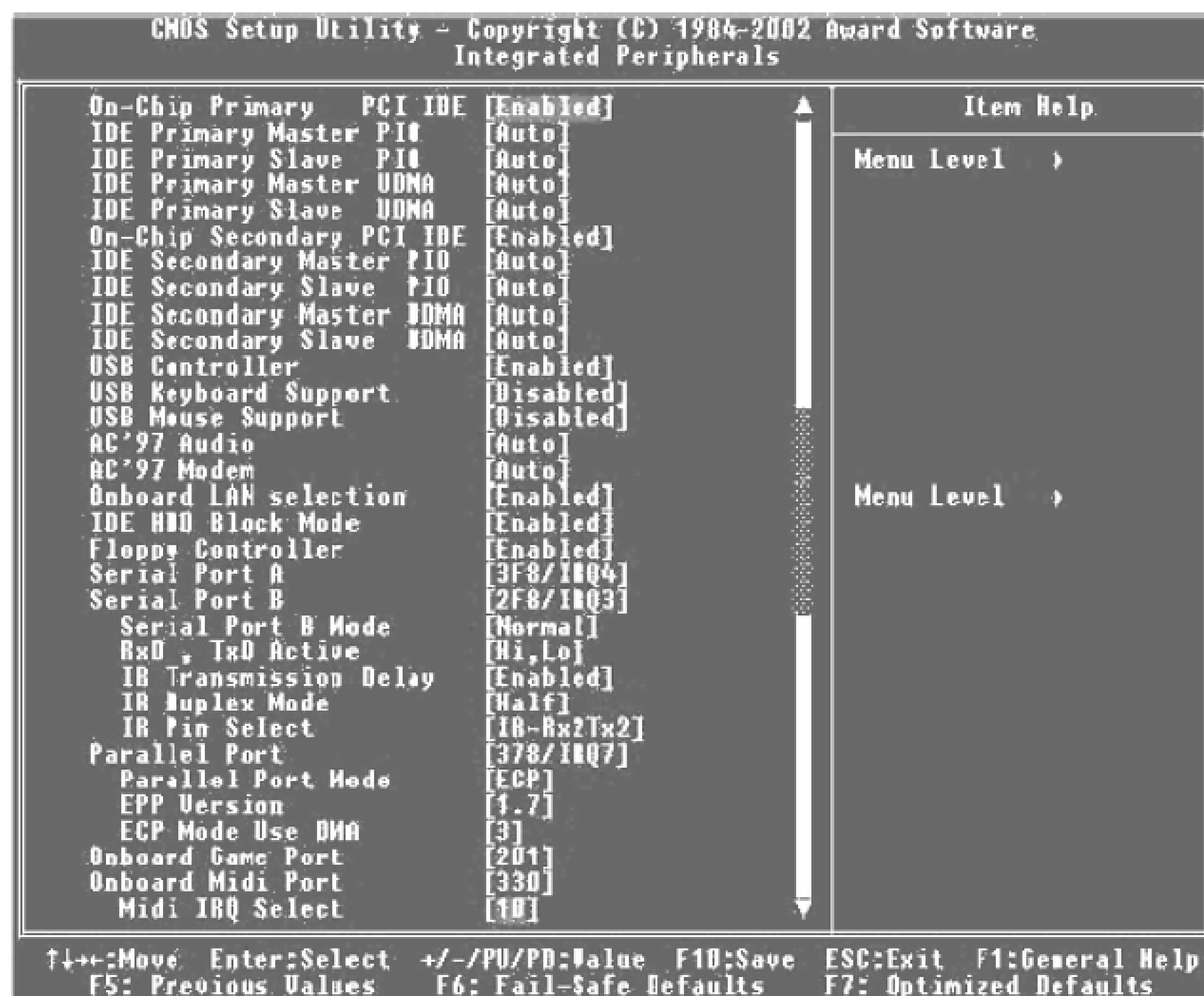


图 5-56　载入主板 BIOS 出厂设置界面

9）SUPERVISOR PASSWORD（管理者密码）

用于设置计算机管理员进入 BIOS 修改设置的密码。

10）USER PASSWORD（用户密码）

用于设置用户的开机密码。

11）IDE HDD AUTO DETECTION（自动检测 IDE 硬盘类型）

用于自动检测本计算机的硬盘容量和类型等信息。图 5-57 所示为自动检测 IDE 硬盘类型设置界面。

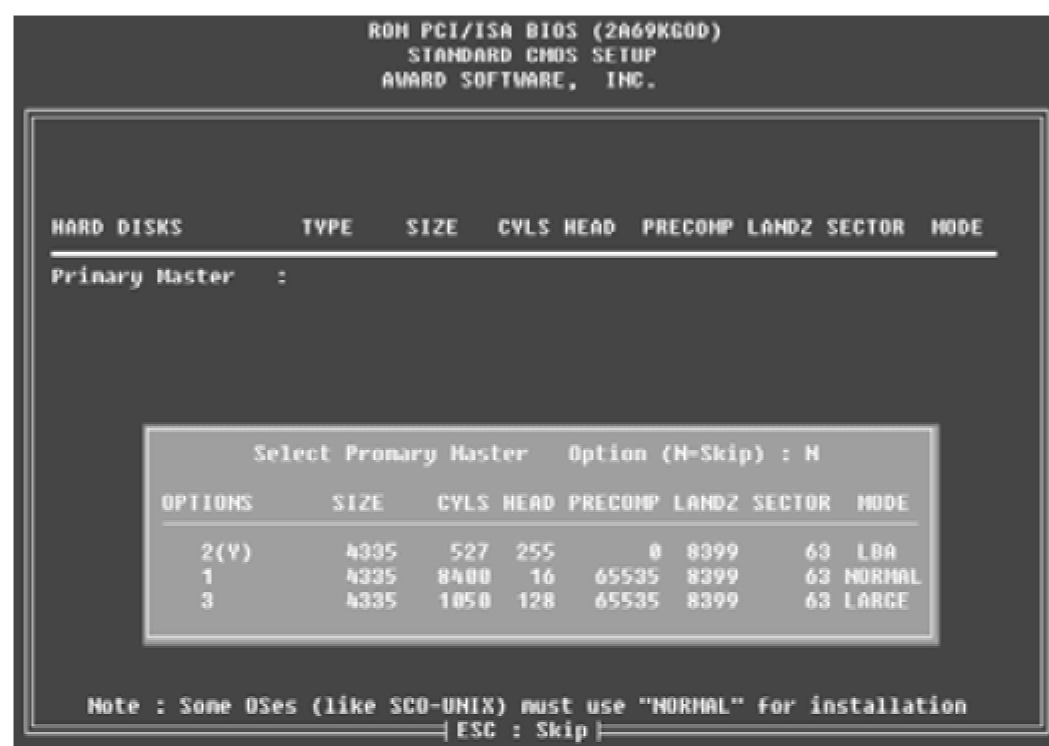


图 5-57　自动检测 IDE 硬盘类型界面

12）SAVE&EXIT SETUP（保存并退出设置）

用于保存已经更改的设置，并退出 BIOS 设置。

13）EXIT WITHOUT SAVE（沿用原有设置并退出 BIOS 设置）

该菜单项表示不保存已经修改的设置，并退出 BIOS 设置。

5.6.2 常见 BIOS 故障及其解决方案

1. BIOS 不能设置

【故障表现】：计算机开机后进入 BIOS 程序，除了可以设置【USER PASSWORD】、【SAVE&EXIT SETUP】和【EXIT WITHOUT SAVE】外，其他各项都不能进入。

【故障分析】：此故障估计是 CMOS 被破坏了，可以尝试放电处理。如果放电后仍不能解决故障，可以尝试升级 BIOS，具体方法可以参照上一节的操作步骤。升级后故障依然存在。

【故障处理】：经分析可以判断是 CMOS 存储器出了问题，换一个新的存储器后，故障排除。

2. BIOS 感染病毒导致计算机不能启动

【故障表现】：一台计算机开机后显示器黑屏，无法正常启动。

【故障分析】：病毒是比较常见的故障因素，计算机可能中了各种各样的病毒。将硬盘取下，挂到正常的计算机上杀毒，终于查杀到病毒，杀毒后重新将硬盘安装好，启动计算机后故障依然存在，此时可以初步判断是 BIOS 芯片中的数据被病毒损坏了。

【故障处理】：排除故障的具体操作步骤如下。

01 打开机箱，用螺丝刀取下 BIOS 芯片，用系统盘启动另外一台主板型号相同的计算机，在启动的过程中按下 Del 键进入 BIOS 启动界面。

02 在 BIOS 设置中将 System BIOS Cache 选项设置为 Enable，保存设置后退出 BIOS 界面。

03 重新启动计算机，用刚才的启动盘启动计算机进入 DOS 环境。当界面出现“A:\”提示符后，取出主板上的 BIOS 芯片，将受损 BIOS 芯片插入到主板 BIOS 的插座上。在此过程中不可断电，否则会导致 BIOS 的数据更新失败。

04 在“A:\”提示符下输入“aflsh”命令后按下 Enter 键，然后根据提示一步步进行操作即可完成 BIOS 的刷新工作。接下来将刷新后的 BIOS 芯片重新插入故障计算机中。

05 启动故障计算机，按下【Del】键进入到 BIOS 启动界面，由 BIOS 自动检测硬盘数据后退出。

06 重新启动计算机，计算机运行正常，故障消失。

5.7 专家答疑

（1）软件不能卸载干净怎么办？

对于计算机高手来说，手工清理注册表是最有效最直接的清除注册表垃圾的方法。手工清理注册表的具体操作步骤如下。

01 利用上述方法打开【注册表编辑器】窗口。

02 在左侧的窗格中展开并选中需要删除的项，选择【编辑】➤【删除】命令，或右击，在弹出的快捷菜单中选择【删除】命令。

03 弹出【确认项删除】对话框，提示用户是否确实要删除这个项和所有其子项，如图 5-58 所示。单击【是】按钮，即可将该项删除。

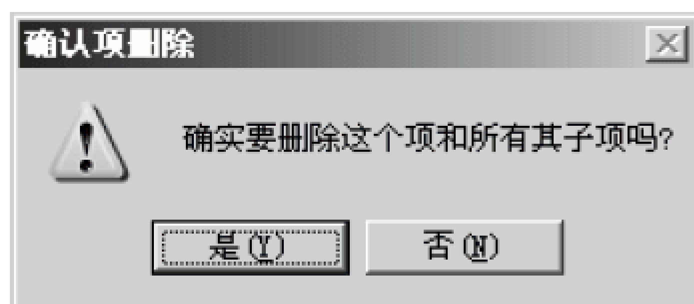


图5-58 【确认项删除】对话框

（2）按一次键，出现多个重复字母怎么办?

【故障现象】：在键盘上按下一个键，出现多个字母。

建议采用如下步骤进行处理。

01 先查看键盘上的按键按下后是否能够正常弹起，如果不能正常弹起，说明键盘已经老化或按键损坏，需要对键盘进行清洗，更换老化的按键。

02 如果键盘按键能够正常弹起，则有可能是键盘按键重复延迟时间过短。单击【开始】按钮，在弹出的【开始】菜单中选择【控制面板】命令。

03 在弹出的【控制面板】中选择【键盘】选项，如图 5-59 所示。



图5-59 选择“键盘”

04 弹出【键盘 属性】对话框，选择【速度】选项卡，然后调整【重复延迟】滑块，使时间稍微长一点即可，如图 5-60 所示。



图 5-60 【键盘 属性】对话框

第 6 章　企业服务器管理与维护

随着全球互联网技术的不断提高、普及，大多数企业对网络信息化办公的依赖越来越大。在企业中用于实现信息化办公的关键设备就是服务器，它可以满足企业信息的存储、对外发布，以及企业相关业务的处理，所以对于企业来说服务器显得越来越重要，服务器的管理维护工作也逐渐得到重视。

本章将介绍基础的服务器管理与维护技术，如服务器的选型与安装、服务器的日常管理操作、常用 DHCP 服务器的管理、打印机服务器的管理等内容。

6.1　企业服务器管理概述

在实施企业服务器管理之前，首先要了解服务器管理的相关知识。

1. 服务器的概念

服务器是指用于管理资源并为用户提供服务的计算机软件。服务器其实和平时家庭使用的计算机操作系统相似，只是它相对于普通计算机系统来说，需要具备更高的稳定性、安全性及性能。所以，通常服务器会采用专门的计算机硬件，这些硬件需要具备远远高出家庭计算机的性能，高端的 CPU、芯片组、内存、磁盘系统和网络等硬件要求，还具有更好的温度、湿度等外部环境保障。

鉴于它对硬件的独特要求，很多厂商也纷纷研发专用的服务器硬件设备，如 IBM、浪潮、中兴等厂商的服务器设备。

2. 服务器的分类

在进行服务器划分时，可以根据其生成厂商、操作系统类型、应用功能等进行分类。

按照系统类型可分为：Windows Server 2003/2008 操作系统、Linux 操作系统和 UNIX 操作系统。

按照应用功能可分为：文件服务器、邮件服务器、Web 服务器、DNS 服务器和代理服务器等。

按照厂商可分为：微软的 Windows 系列、红旗和红帽的 Linux 系列、IBM 的 UNIX 系列等。

6.2 服务器的选型与安装

服务器的选择，需要考虑设备的可用性、可靠性、稳定性和 I/O 吞吐能力等性能特征，结合需求选择完成后，还需要依照不同类型服务器的特征进行安装和初始化操作。本节将详细介绍服务器的选型、压力测试及安装方法等内容。

6.2.1 服务器的选型

服务器选型时需要考虑可用性、可靠性、稳定性和 I/O 吞吐能力等性能特征，下面对此进行简要说明。

服务器选择时要考虑功能可用性。为了更好地实现某种服务功能，服务器在设计时会针对不同的功能进行强化设计，如强化 Web 发布功能的 Web 服务器，强化数据存储管理的存储服务器。不同的服务器对于硬件的处理能力要求各有不同，如 Web 服务器对硬盘大小的要求和存储服务器对硬盘大小的要求是截然不同的。所以在选择时要慎重考虑服务器对软硬件性能的要求，要确保搭建的服务器能够满足应用功能的需求。

服务器作为重要的信息服务、存储设备，需要确保其安全有效的应用。如果服务器本身的安全级别或安全设置有限，是无法提供可靠应用的。

为了确保服务器可持续性的使用，需要提供磁盘、风扇、电源等的冗余机制。同时还要在故障恢复方面有独特的技术保障，如服务器性能监控管理平台。

结合以上内容介绍几个典型的服务器选型分析案例。

1. 文件服务器

文件服务器主要为客户机提供文件上传、下载，对于服务器本身来说对读写能力的要求比较高，所以需要考虑 I/O 吞吐能力，也就是硬盘的读写能力和内存缓存的要求。一般用户少的话可以增加内存提高缓存；如果用户多的话可以在增加内存的基础上提高磁盘的读写速度，可以通过更换高性能的磁盘或者增加多块磁盘构成磁盘冗余阵列来提高读写速度。

2. 数据库及应用服务器

这类服务器对 CPU 的处理能力、内存的缓存能力和 I/O 吞吐能力要求比较高，所以在选择时要着重考虑这三个方面。通常用于大中型企业、重要行业、政府关键部门等应用领域。

3. Web 应用服务器

这类服务器主要用于对外发布网站网页。如果主要用于发布静态网页需要具有较高的内存缓存空间；如果用于发布基于 ASP、Java、PHP 等动态网站，在发布时服务器需要进行大量的动态网站访问请求，所以除了内存的要求外，还应当配置较高的 CPU 处理能力。

4. 部门办公服务器

一般部门服务器主要用于部门间的文件存储管理或者打印管理，这类服务器对性能的要求相对较低，所以采用一般的配置即可。

综上所述，服务器的选型要考虑多方面的性能需求。但是考虑信息技术的发展速度，在进行采购时还应当考虑服务器的扩展性，确保服务器在今后几年内依然能够满足需求，或者有较好的升级空间。

6.2.2 服务器的压力测试

所谓服务器的压力测试，就是测试服务器的工作能力。在服务器搭建好之后最迫切要获得的信息就是服务器的工作能力，如能够承载多大的用户访问量、访问请求的响应速度和容错能力等性能。

市场上使用的服务器压力测试工具比较多，很多服务器厂商针对自己的产品也都有对应的服务器压力测试程序。下面以 Windows 环境下的 Apache Web 服务器为例进行介绍。

在 Apache 服务器中自带了一个测试程序 ab.exe，这个程序可以用来测试能够承载的请求数、响应速度等性能，具体操作方法如下。

该程序需要使用命令行在 apache 程序根目录下执行命令，命令格式如下。

```
ab -c 请求数 -n 线程数 网址
```

说明：配置的线程数不宜过大，依计算机的承受能力而定。网址需要制定目标网页文件名。

例：测试 Apache 服务器 192.168.1.101 的访问性能。

切换至 apache 应用程序根目录配置命令如下。

```
C:Apachebin>ab -c 100 -n 100 http://192.168.1.101/index.html
Benchmarking 192.168.1.101 (be patient).....done
Server Software: Apache/2.0.63                                      //目标 Apache 服务器版本号
Server Hostname: 192.168.1.101                                      //目标服务器地址或主机头名称
Server Port: 80                                                     //目标网址发布端口
Document Path: /index.html                                          //目标网页相对地址
Document Length: 302 bytes                                          //目标网页大小
Concurrency Level: 100                                              //测试的并发线程数
Time taken for tests: 1.140625 seconds                              //测试使用时间
Complete requests: 100                                              //成功的请求数
Failed requests: 0                                                  //失败的请求数
Write errors: 0                                                     //发送错误数
Total transferred: 60500 bytes                                      //测试使用总流量
HTML transferred: 3020 bytes                                        // HTML 文件使用的流量
Requests per second: 69.21 [#/sec] (mean)                           //平均每秒请求数
Time per request: 138.523 [ms] (mean)                               //平均每秒响应时间
Time per request: 13.825 [ms] (mean, across all concurrent requests) //平均每秒请求时间
Transfer rate: 36.15 [Kbytes/sec] received                          //平均传输速率
……
```

6.2.3 安装 Windows Server 2008 的准备工作

安装 Windows Server 2008 的方法主要有两种，通过 Windows Server 2003 升级安装，或者全新安装。无论哪一种安装方式，在安装之前都要做好一些准备工作，具体准备工作如下。

1. Windows Server 2008 的系统要求

这里主要考虑的是系统安装的硬件要求，如表 6-1 所示。

表 6-1　Windows Server 2008 系统的硬件要求

组件	要求
内存	512MB 以上，最好为 2GB 或更高
处理器	1GHz 以上，推荐使用 2GHz 或更快
可用磁盘空间	最低 10GB，建议系统分区在 20GB 以上

以上要求只限于参考，目前大部分主机都可以满足 Windows Server 2008 的安装需求。

2. 规划 Windows Server 2008 的安装

解决硬件配置需求后，还需要进行安装的规划，主要有以下几点内容。

（1）确定是升级安装还是全新安装。一般正在运行关键业务程序的服务器要将原有重要数据信息备份，然后进行升级安装。

（2）确定在计算机上是安装单系统还是安装多系统。大多数主机会安装单系统，无论安装哪种系统都需要为其分配独立的主分区。

（3）确定磁盘分区文件系统类型。Windows Server 2008 默认使用 NTFS。

（4）规划服务器所需要提供的服务。

（5）确定服务器管理员账户的密码。

6.2.4　项目实战 1：安装 Windows Server 2008 操作系统

安装 Windows Server 2008 操作系统的方法比较简单，具体操作步骤如下。

01 在服务器中放入 Windows Server 2008 安装光盘，启动计算机。如果计算机没有读取光盘，可以设置 BIOS 启动顺序，使其优先启动光盘。计算机启动后读取安装光盘，打开【安装 Windows】窗口，在该窗口可以设置【要安装的语言】、【时间和货币格式】、【键盘和输入方法】等信息，建议采用默认配置，单击【下一步】按钮，如图 6-1 所示。

02 弹出如图 6-2 所示的窗口，窗口左下角有【安装 Windows 须知】和【修复计算机】两个选项可以选择，单击【现在安装】按钮，开始 Windows Server 2008 操作系统的安装。



图 6-1　【安装 Windows】窗口



图 6-2　【现在安装】窗口

03 弹出【选择要安装的操作系统】对话框，Windows Server 2008 提供了 6 种系统安装选项，

选择【Windows Server 2008 Enterprise（完全安装）】选项，单击【下一步】按钮，如图 6-3 所示。

04 弹出【请阅读许可条款】对话框，选中【我接受许可条款】复选框，单击【下一步】按钮，如图 6-4 所示。

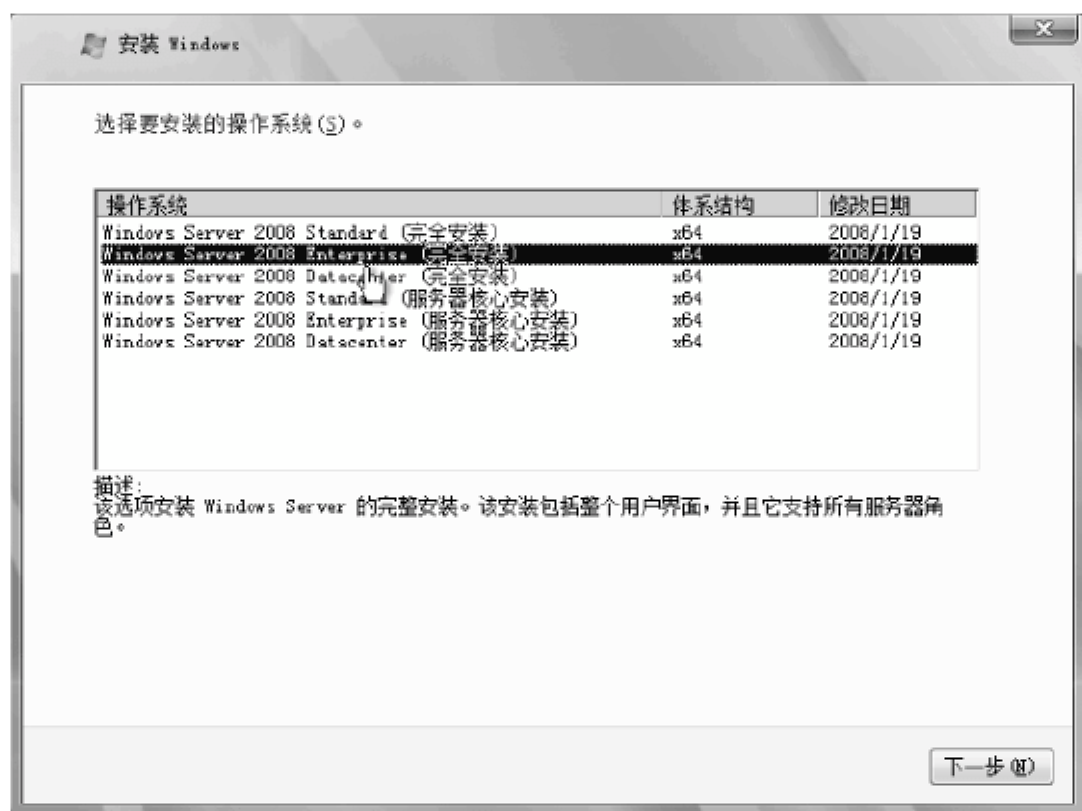


图 6-3 【选择要安装的操作系统】对话框

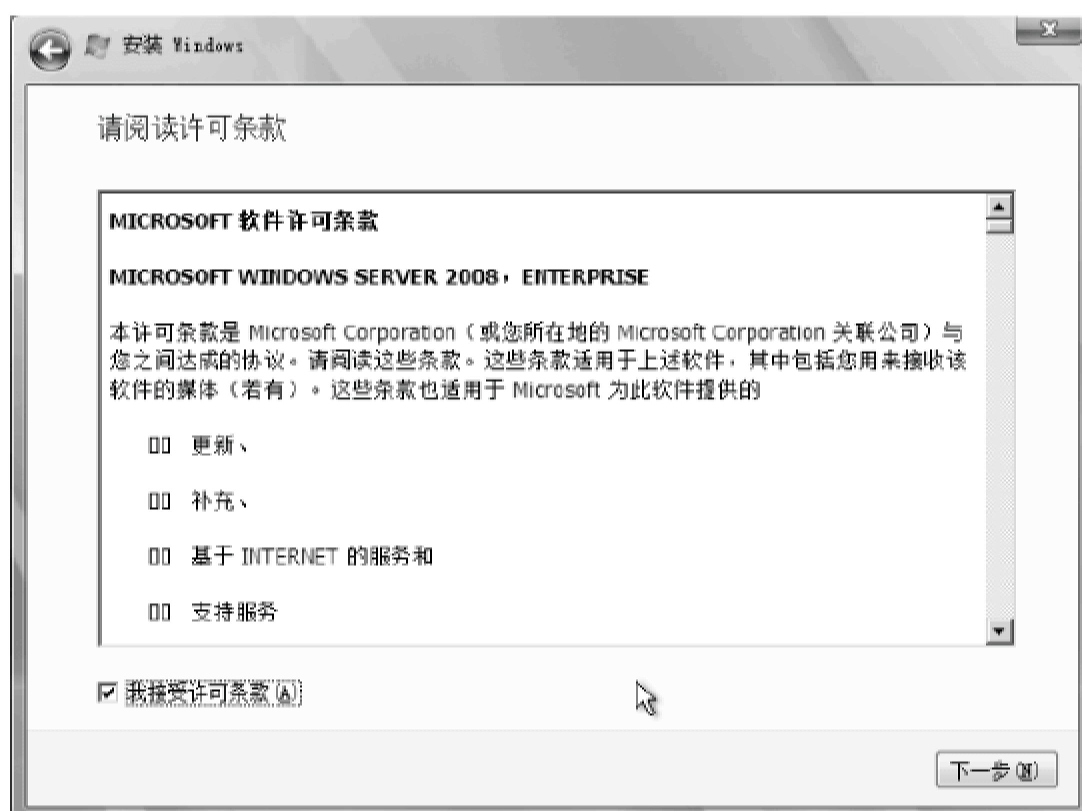


图 6-4 【请阅读许可条款】对话框

05 弹出【您想进行何种类型的安装】对话框，因为当前计算机是第一次安装操作系统，所以单击【自定义（高级）】选项，如图 6-5 所示。

06 弹出【您想将 Windows 安装在何处？】对话框，该对话框主要用于指定系统分区，由于是第一次安装，磁盘没有分区，单击【驱动器选项（高级）】选项创建系统分区，如图 6-6 所示。



图 6-5 【您想进行何种类型的安装】对话框

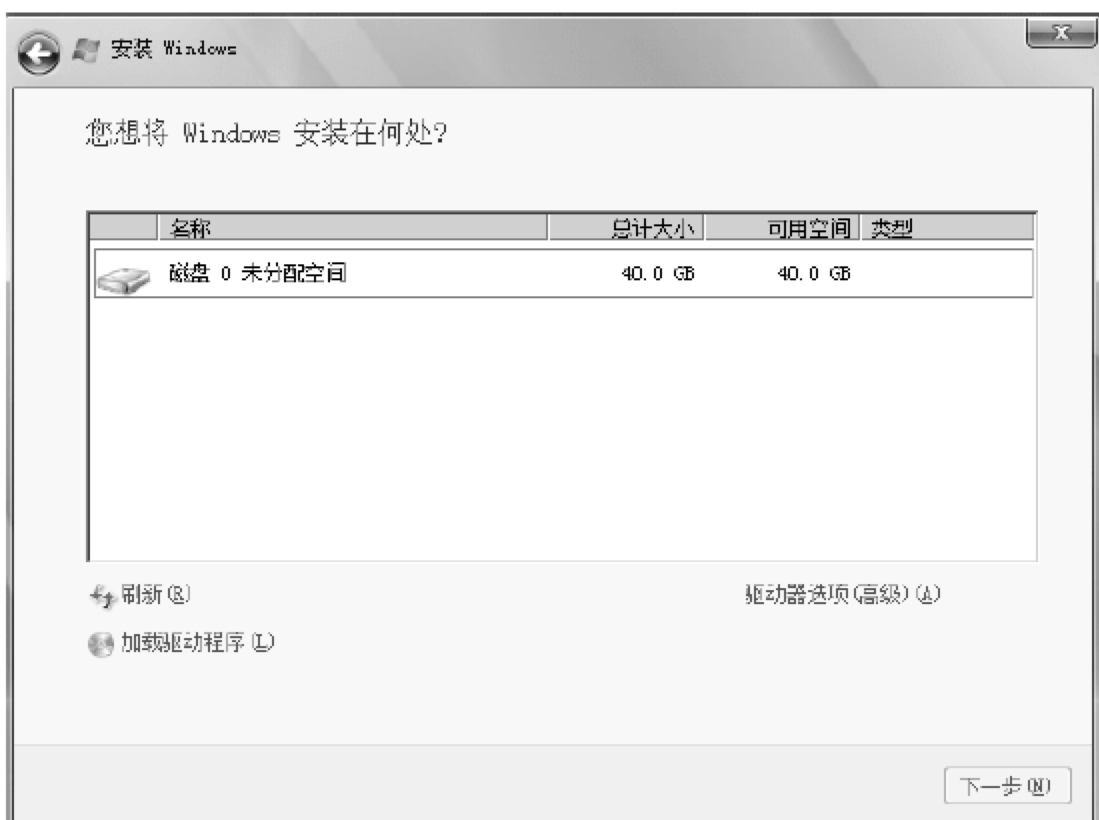


图 6-6 【您想将 Windows 安装在何处？】对话框

07 该对话框下侧工具选项变为分区编辑工具，单击【新建】选项，可显示出【大小】文本框，输入新建分区大小，单击【应用】按钮，如图 6-7 所示。

08 新分区创建成功，本实例将所有磁盘空间创建为一个分区，选中该分区，单击【下一步】按钮，如图 6-8 所示。



图 6-7　划分磁盘分区



图 6-8　系统分区创建成功

09 如图 6-9 所示，弹出【正在安装 Windows】对话框，系统安装时间一般在 10~20 分钟。

10 系统安装完毕后重新启动，并进入登录画面，第一次登录提示更改密码，单击【确定】按钮，如图 6-10 所示。



图 6-9　开始安装 Windows



图 6-10　首次登录提示修改密码

11 显示如图 6-11 所示界面，在两个文本框中分别输入新密码，第二个文本框用于确认密码。建议设置满足安全策略要求的密码，大写字母、小写字母、数字、特殊字符四种元素任选三种，且超过七位。密码输入完成后按【Enter】键确认。

12 显示如图 6-12 所示界面，表示密码修改成功，单击【确定】按钮登录操作系统。



图 6-11　修改系统密码



图 6-12　系统密码修改成功

6.3　服务器系统操作基础

本节主要介绍 Windows Server 2008 操作系统的基本管理操作，包括任务管理器的使用、用户和组的管理、组策略的安全配置、系统服务和端口的管理等内容。

6.3.1　利用任务管理器查看系统运行状态

任务管理器是 Windows 系统自带的一种查看系统运行状态的工具，可以用来查看系统当前运行的程序、进程、CPU 和内存使用情况、网络流量、登录账户等信息。具体内容介绍如下。

01　右击桌面下侧的任务栏，在弹出的快捷菜单中选择【任务管理器】命令，如图 6-13 所示。

02　打开【Windows 任务管理器】窗口，窗口主要由【应用程序】、【进程】、【服务】、【性能】、【联网】和【用户】6 个选项卡组成。首先选择【应用程序】选项卡，该选项卡显示了当前系统打开的任务窗口，选中某一任务名，单击【结束任务】按钮可将其关闭，也可以单击【新任务】按钮添加新的任务程序，如图 6-14 所示。

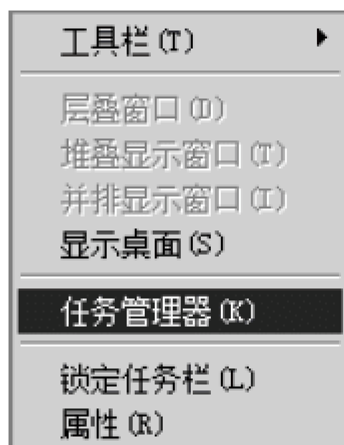


图 6-13　任务栏快捷菜单



图 6-14　【任务管理器】窗口

03 选择【进程】选项卡，该选项卡显示了当前系统运行的进程列表，以及各个进程的执行用户名、CPU 占有率、内存使用量及描述信息。选择某一进程名，单击【结束进程】按钮可将其关闭，如图 6-15 所示。使用此方法可以强制关闭无法关掉的程序，同时也可以关闭无用或者不认识的进程以减少系统资源的消耗和木马等不安全程序的后台执行。

04 很多进程的运行文件不好找到，可以通过选择【文件】➢【新建任务（运行...）】命令进行添加，如图 6-16 所示。例如 explorer.exe（桌面环境运行程序），当系统桌面卡死之后，可以将该进程结束然后重新添加，以恢复桌面显示。



图 6-15　【进程】选项卡



图 6-16　【新建任务】命令

05 选择【服务】选项卡，该选项卡主要显示系统正在运行或者停止运行的服务，可单击【服务】按钮打开系统的【服务】管理工具，进而修改系统服务的运行状态，如图 6-17 所示。

06 选择【性能】选项卡，该选项卡用于显示 CPU 和内存的使用情况，是查看系统当前运行性能的主要方法之一，如图 6-18 所示。



图 6-17　【服务】选项卡



图 6-18　【性能】选项卡

07 选择【联网】选项卡，该选项卡用于显示主机网卡的流量，显示的是当前流量占总带宽的百分比，用于查看服务器的网络访问流量，如图 6-19 所示。

08 选择【用户】选项卡，该选项卡用于显示登录当前服务器系统的用户信息，包括本地交互登录和远程登录的用户，如图 6-20 所示。可以通过该选项卡发现远程用户非法登录系统。

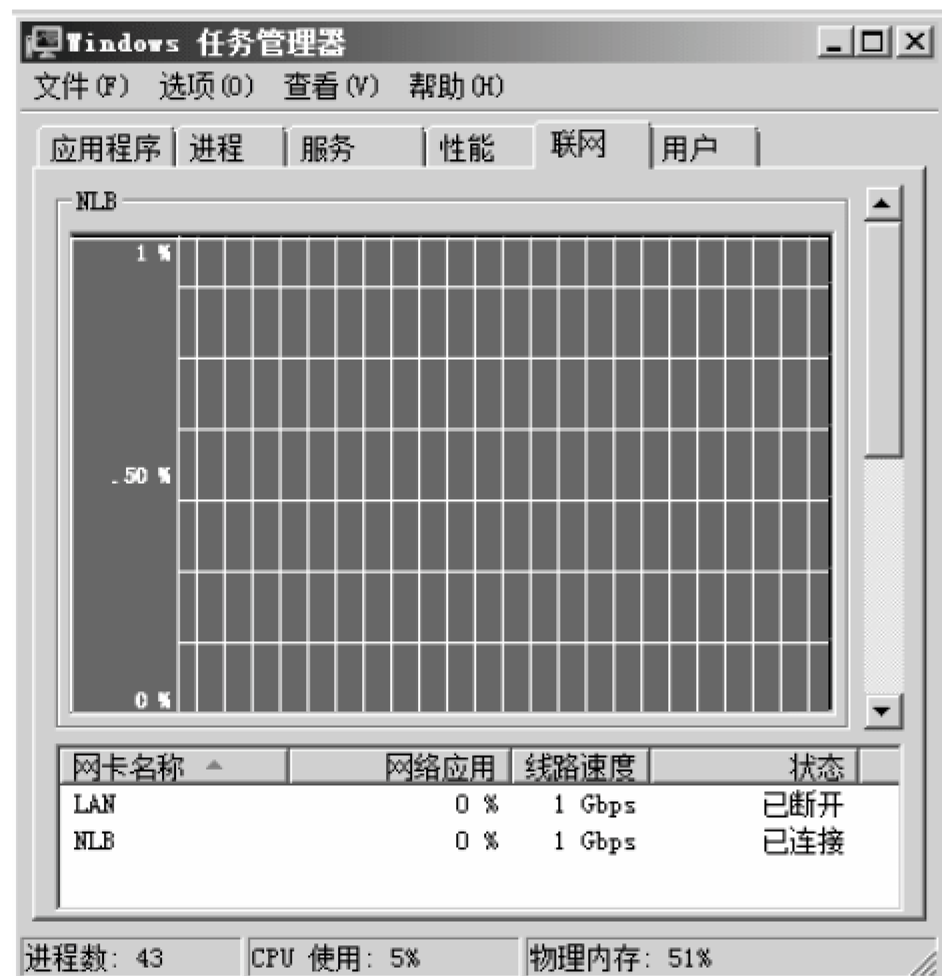


图 6-19 【联网】选项卡



图 6-20 【用户】选项卡

6.3.2 本地用户和组分配与权限管理

用户和组的管理是操作系统管理的重要组成部分，主要是为交互登录或远程访问提供有效账户，并赋予严格有效的访问权限。

1. 创建用户和组

创建用户和创建组的方式相似，下面以创建用户为例进行演示。

01 右击【我的计算机】图标，在弹出的快捷菜单中选择【管理】命令，如图 6-21 所示。

02 弹出【服务器管理器】窗口，在左侧选项列表中选择【配置】➢【本地用户和组】➢【用户】选项，在【用户】窗格空白处右击，在弹出的快捷菜单中选择【新用户】命令，如图 6-22 所示。



图 6-21 【我的计算机】快捷菜单

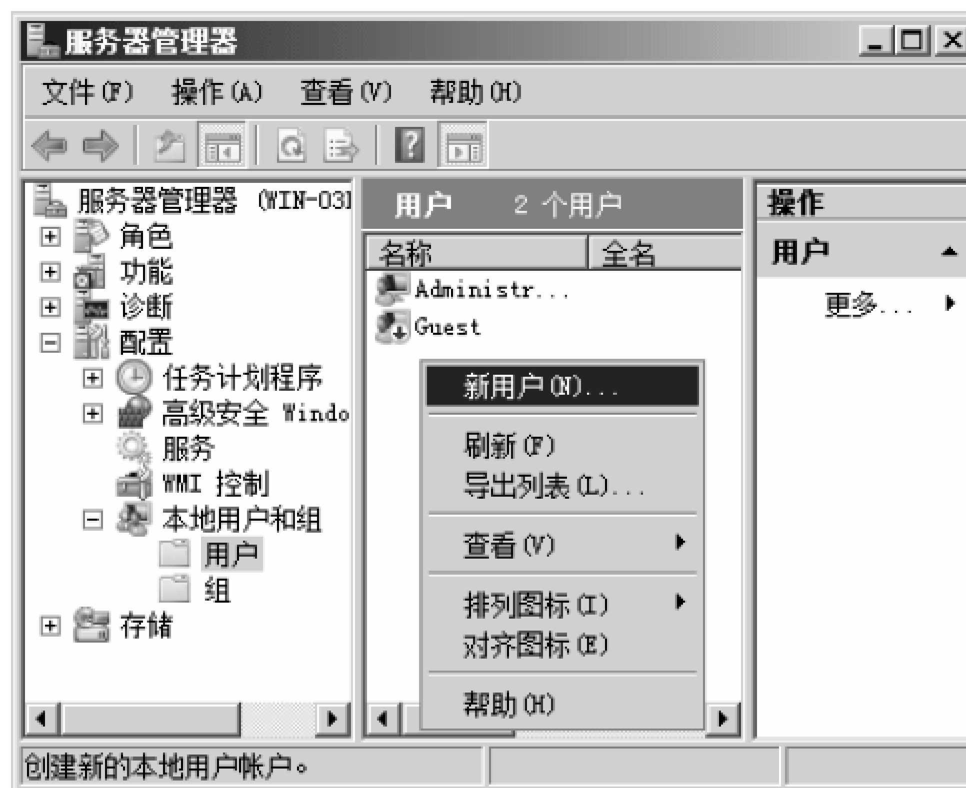


图 6-22 【服务器管理器】窗口

03 弹出【新用户】对话框，在【用户名】、【密码】和【确认密码】文本框中输入相关内容，本实例创建用户为“user1”，选中【用户不能更改密码】和【密码永不过期】复选框，单击【创建】按钮，如图 6-23 所示。

04 新用户添加成功，返回【用户】窗格，如图 6-24 所示。



图 6-23 【新用户】对话框



图 6-24 新用户添加成功

05 对已经存在的用户可以定期更改其密码，以确保账户安全。右击用户名，在弹出的快捷菜单中选择【设置密码】命令，如图 6-25 所示。

06 弹出【为 Administrator 设置密码】对话框，单击【继续】按钮，如图 6-26 所示。



图 6-25 更改用户密码

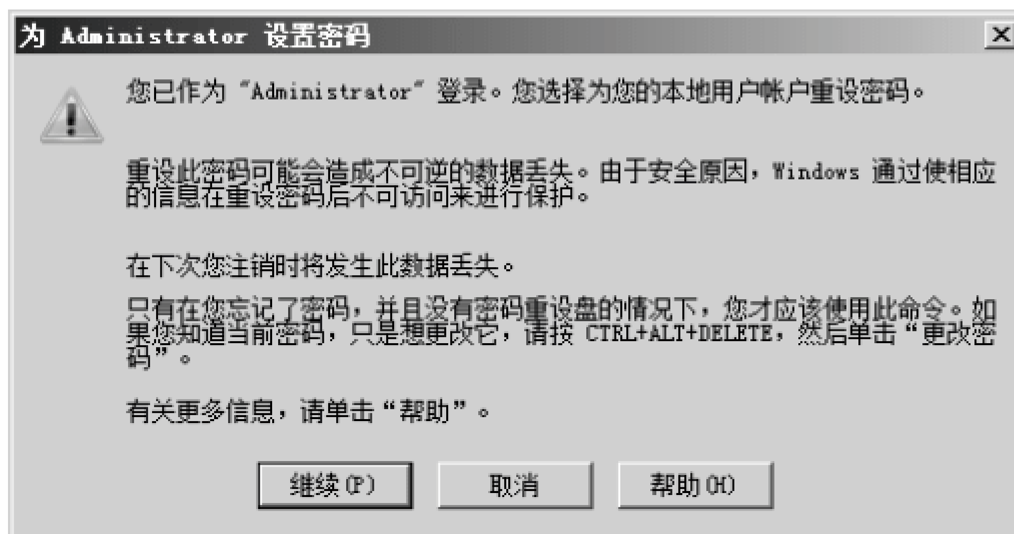


图 6-26 【为 Administrator 设置密码】对话框

07 弹出新对话框，在【新密码】和【确认密码】文本框中输入新设密码，单击【确定】按钮，如图 6-27 所示。

08 弹出【本地用户和组】对话框，单击【确定】按钮，完成密码修改，如图 6-28 所示。

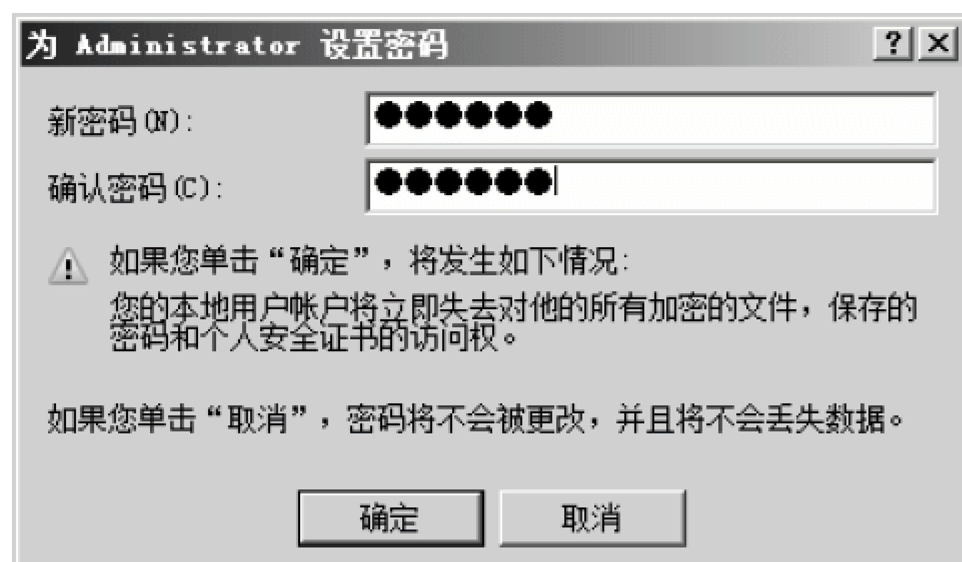


图 6-27　设置新密码

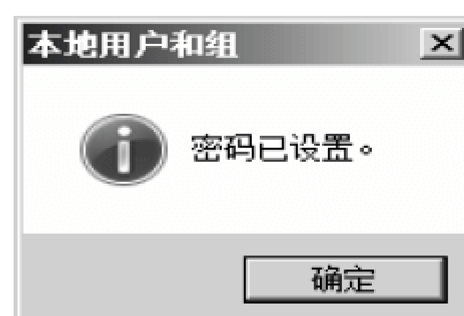


图 6-28　【本地用户和组】对话框

2. 为用户和组分配文件访问权限

在 Windows Server 2008 中用户和组的权限主要通过对文件或目录进行指派得以体现。具体操作方法如下。

01 选择一个文件或目录右击，在弹出的快捷菜单中选择【属性】命令，如图 6-29 所示。

02 弹出属性对话框，选择【安全】选项卡，显示了当前对该文件有操作权限的用户和组，并在权限列表中显示了对应权限，单击【编辑】按钮，可编辑用户和组的权限，如图 6-30 所示。

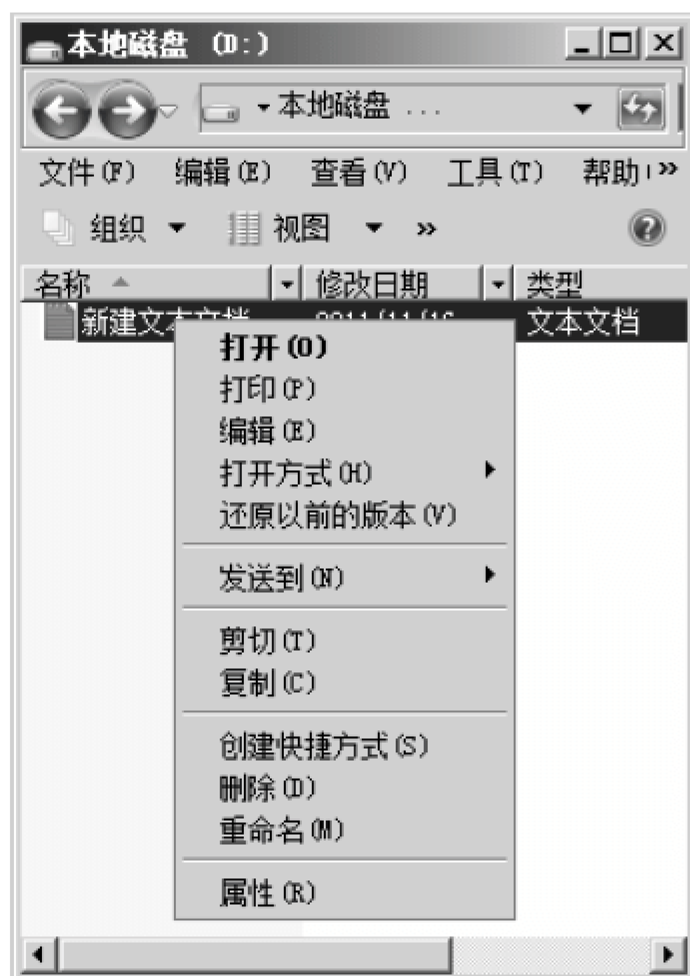


图 6-29　文件或目录的快捷菜单

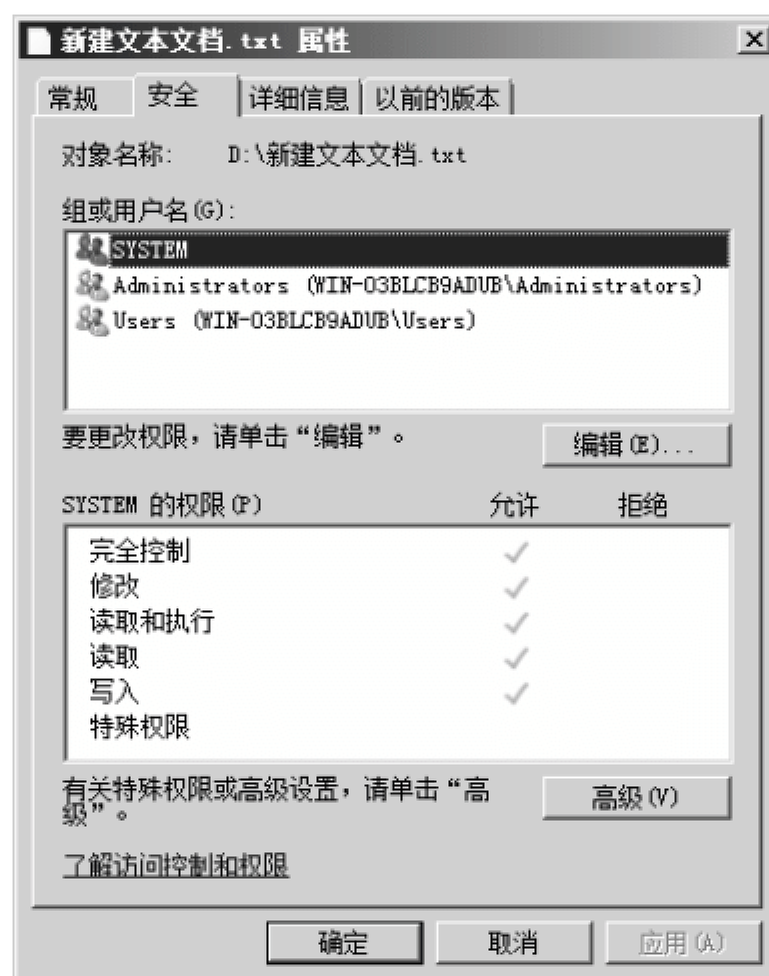


图 6-30　文件或目录【属性】对话框

03 在弹出的对话框中选择 Administrators 组，下方显示了 Administrators 组的权限，通过选中【允许】或【拒绝】选项下的复选框调整权限，如果对该文件添加新用户的访问权限，可以单击【添加】按钮，如图 6-31 所示。

04 弹出【选择用户或组】对话框，可在文本框中直接输入用户或组名进行添加，如"user1"；如果不确定用户或组名可单击【高级】按钮进行添加，如图 6-32 所示。

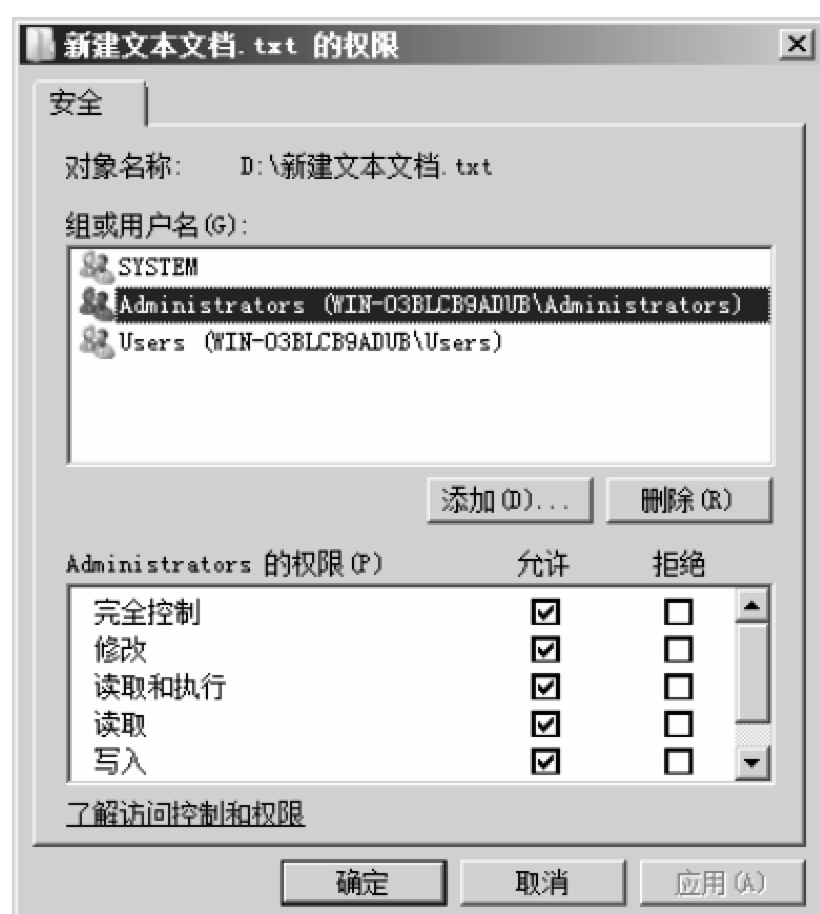


图 6-31　权限对话框 1



图 6-32　【选择用户或组】对话框 1

05 弹出高级选项内容，单击【立即查找】按钮，在搜索结果选项列表中会显示当前主机存在的所有用户和组名，选择需要的用户和组名单击【确定】按钮，如图 6-33 所示。

06 用户或组选择成功，单击【确定】按钮，如图 6-34 所示。

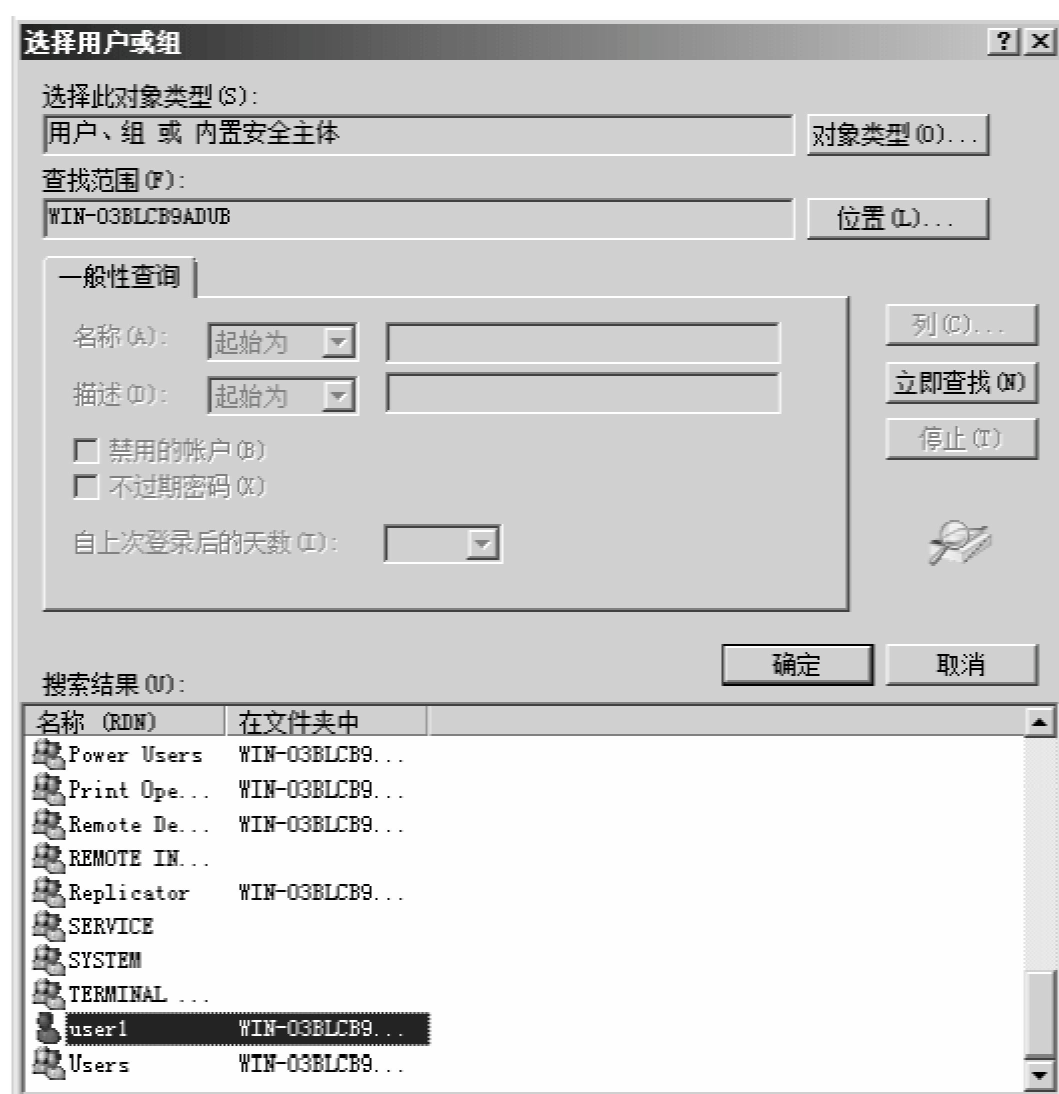


图 6-33　【选择用户或组】对话框 2



图 6-34　选择用户成功

07 用户添加成功，选择已添加的用户，在下侧修改其权限，单击【确定】按钮完成权限的配置，如图 6-35 所示。

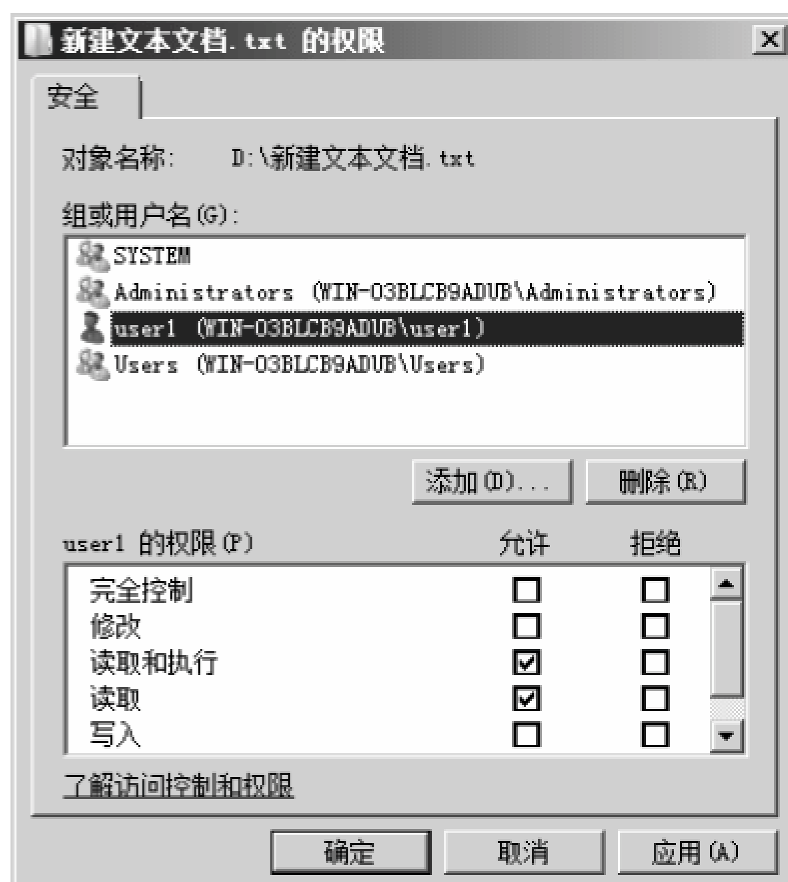


图 6-35　权限对话框 2

6.3.3　项目实战 2：配置组策略提高系统安全

组策略可以用来配置计算机运行环境及安全策略，包括本地策略、安全设置等，可以通过以下方式打开组策略的配置程序。

01 选择【开始】➢【运行】选项，弹出【运行】对话框，在【打开】文本框中输入“gpedit.msc”命令，单击【确定】按钮，如图 6-36 所示。

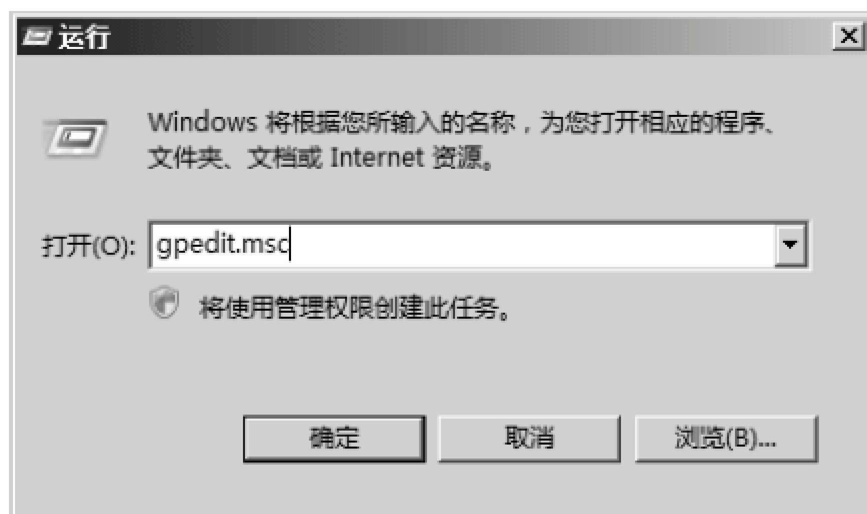


图 6-36 【运行】对话框

02 弹出【本地组策略编辑器】窗口，窗口左侧显示了可编辑的选项列表，主要有【计算机配置】和【用户配置】两块内容，如图 6-37 所示。【计算机配置】用来定义计算机全局的策略内容，【用户配置】用来定义用户操作环境的配置内容，针对计算机的全局安全配置主要在【计算机配置】选项页中完成。

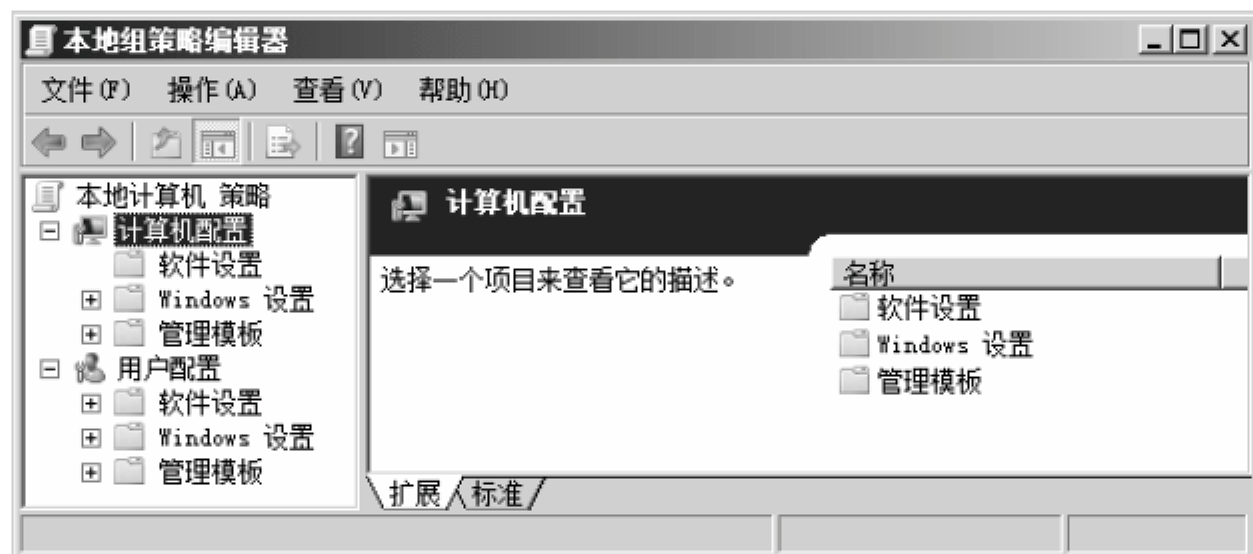


图 6-37 【本地组策略编辑器】窗口

组策略的配置内容比较多，下面列举一些常规配置，具体内容如下。

1. 账户策略

账户策略主要包括密码策略和账户锁定策略。

01 在左侧列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【账户策略】➢【密码策略】选项，右侧弹出常见的密码策略选项，通过双击选项可进行配置，如图 6-38 所示。

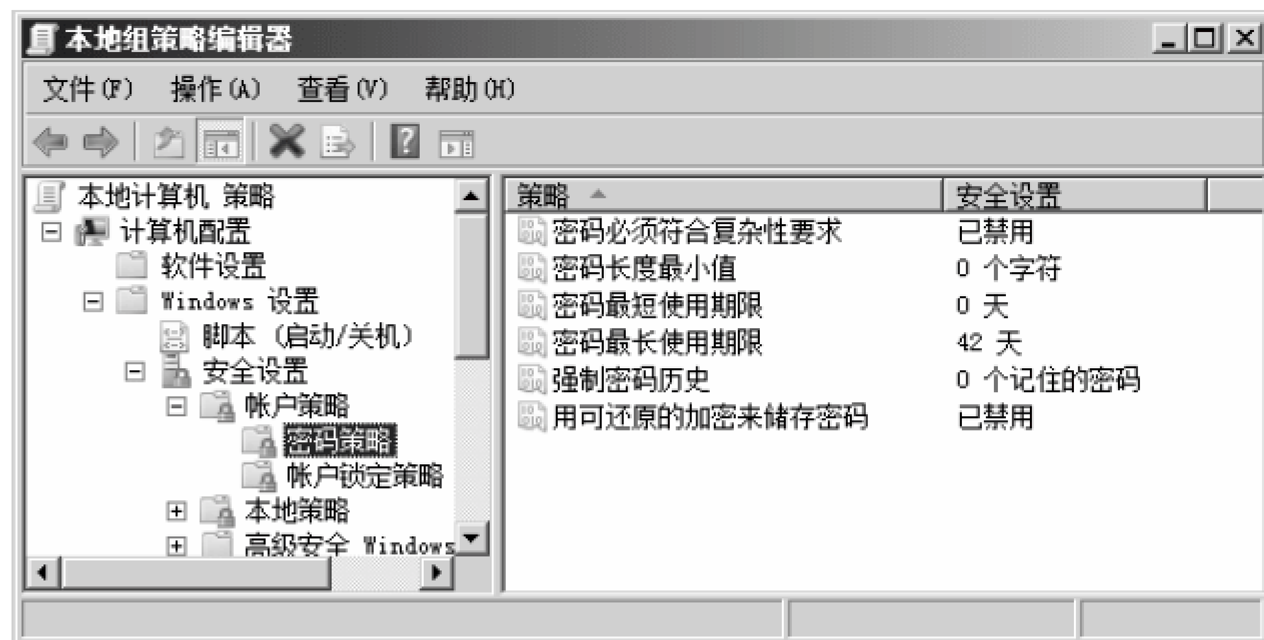


图 6-38　【密码策略】选项页

密码策略选项含义介绍如下。

- 【密码必须符合复杂性要求】：复杂性指由数字、字符和字母三种字符混合而成的不小于一定位数的密码，一般建议服务器开启该功能。
- 【密码长度最小值】：允许使用的密码最小长度，建议设置为 8。
- 【密码最短使用期限】：允许密码使用的最短时间，用于防止在一段时间内密码被恶意改动。
- 【密码最长使用期限】：允许密码使用的最长时间，用于规范管理员周期性地更改密码，这可以使被破解的密码在周期结束后失效，保证登录安全。
- 【强制密码历史】：允许系统记录的历史密码设置数，如果设置为 3，则表示记录之前的三次密码设置记录，新设密码不能和记录的历史密码相同。

02 选择【安全设置】➢【账户策略】➢【账户锁定策略】选项，右侧弹出账户锁定策略选项，双击可打开设置对话框，如图 6-39 所示。

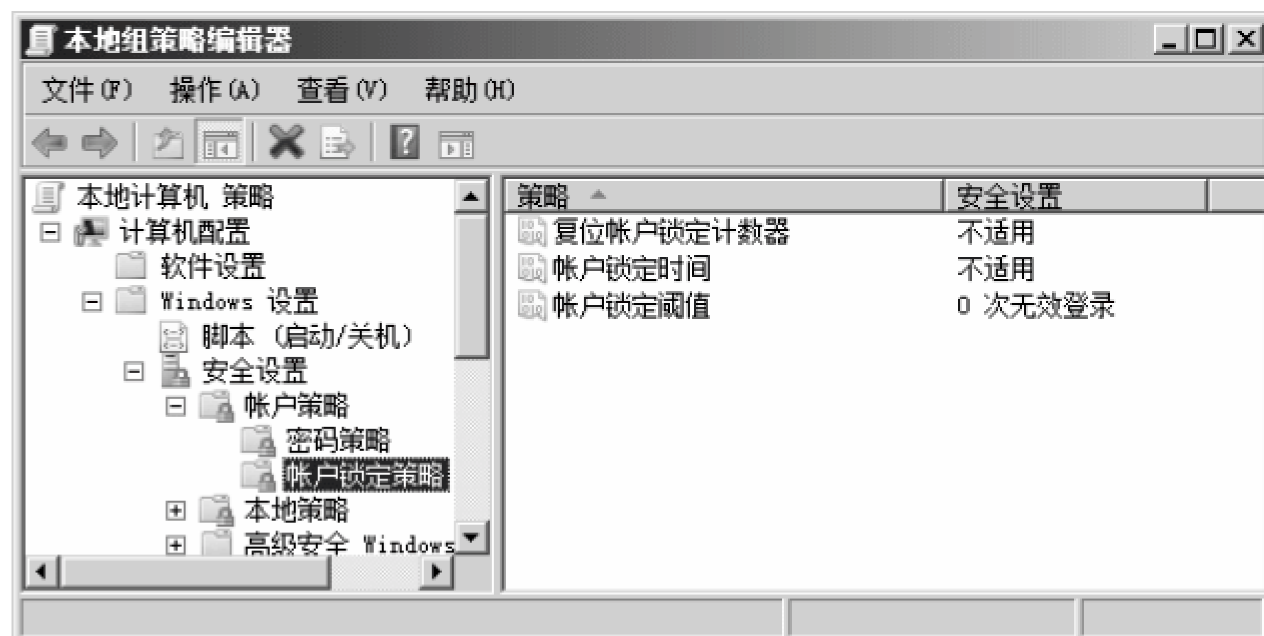


图 6-39　【账户锁定策略】选项

账户锁定策略选项含义介绍如下。

- 【复位账户锁定计数器】：记录错误登录次数的时间范围，如果设置为 30 秒，则只记录连续 30 秒内错误登录的次数。
- 【账户锁定时间】：系统登录被锁后，锁定的时间，一般设置为 30 秒。
- 【账户锁定阀值】：设置使用账户登录系统允许错误输入密码信息的次数，一般设置为 3 次。如果错误登录超过限定次数，系统锁定，需要等待锁定时间自动解锁，或者由系统管理员手工解锁。

2. 本地策略

本地策略主要有审核策略、用户权限分配和安全选项三部分构成，分别介绍如下。

1）审核策略

审核策略用于审核操作系统中的一些重要操作，并在审核策略日志中显示。可以通过审核策略日志查看系统之前发生的事情，对于故障发现和故障恢复有很大的帮助。

01 选择【安全设置】➢【本地策略】➢【审核策略】选项，右侧显示系统审核策略，默认无审核，通过双击策略选项可以打开审核策略配置对话框将其开启，如图 6-40 所示。

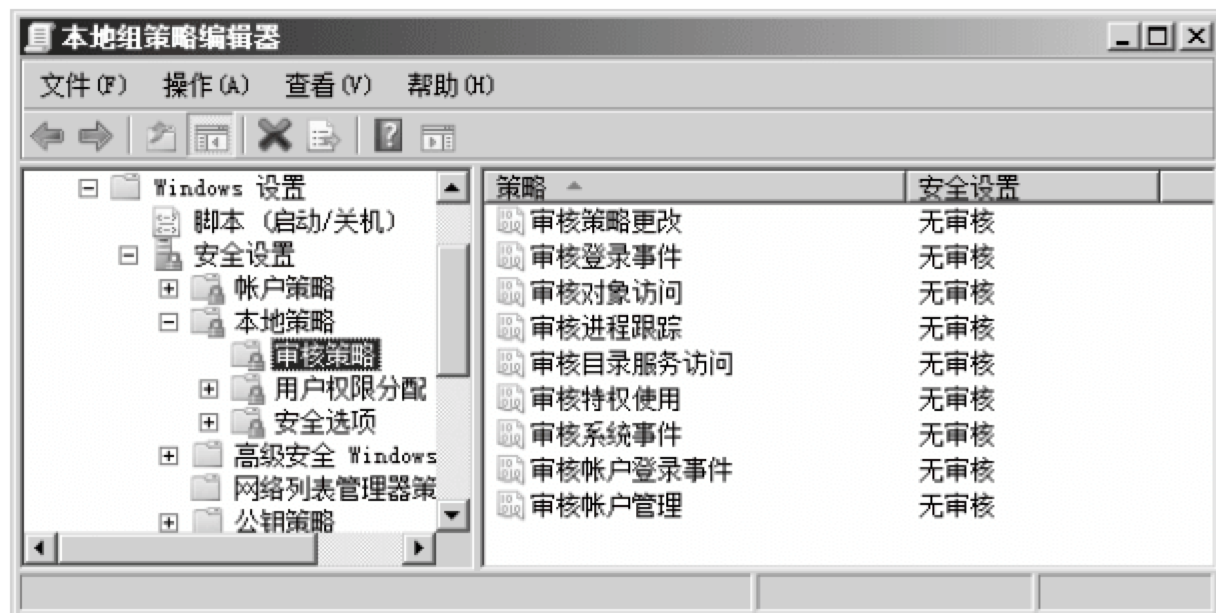


图 6-40 【审核策略】选项

审核策略各选项含义介绍如下。

- 【审核策略更改】：记录所有的系统策略修改内容，并在审核策略日志中显示。
- 【审核登录事件】：记录所有的系统登录事件，并在审核策略日志中显示。
- 【审核对象访问】：记录开启审核功能的文件或目录的访问事件，并在审核策略日志中显示。
- 【审核进程跟踪】：跟踪系统进程，审核其安全合法性，并在审核策略日志中显示。
- 【审核目录服务访问】：审核域环境中目录服务器的访问，并在审核策略日志中显示。
- 【审核系统事件】：审核系统事件日志，并在审核策略日志中显示。
- 【审核账户登录事件】：记录所有的账户登录事件，并在审核策略日志中显示。
- 【审核账户管理】：审核账户的配置和修改，并在审核策略日志中显示。

02 打开【服务器管理器】窗口，在左侧选项列表中选择【诊断】➢【事件查看器】➢【Windows 日志】➢【安全】选项，在右侧【安全】窗格中显示了系统的安全日志，大部分是审核策略日志信

息，可以双击日志记录查看其详细信息，如图 6-41 所示。



图 6-41　【安全】选项

2）用户权限分配

用户权限分配是为不同的账户分配对计算机的各种配置权限。例如，允许某些账户可以更改系统的时间，允许某些账户可以管理审核和安全日志，具体操作方法如下。

01 选择【安全设置】➢【本地策略】➢【用户权限分配】选项，右侧显示了可配置的策略选项，如【从网络访问此计算机】选项，用于指定允许哪些账户可以远程访问该计算机，双击该选项，如图 6-42 所示。

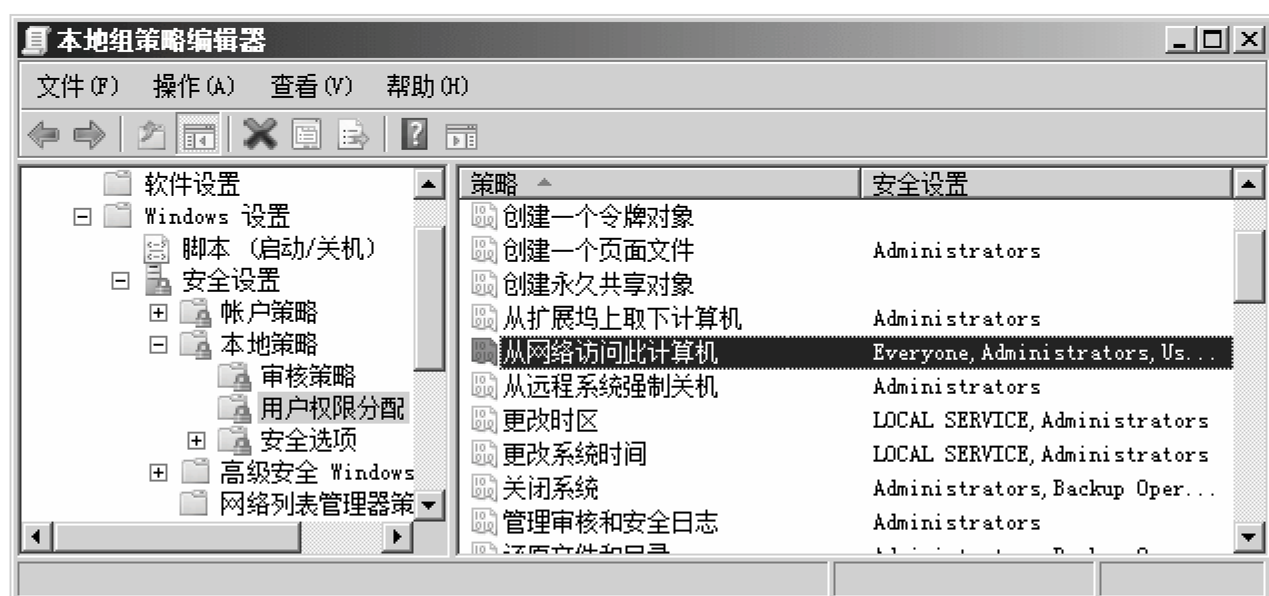


图 6-42　【用户权限分配】选项

02 打开【从网络访问此计算机 属性】对话框，列表中显示了有权限的账户和组，可以单击【添加用户或组】和【删除】按钮进行添加或删除，完成后单击【确定】按钮，如图 6-43 所示。



图 6-43　【从网络访问此计算机 属性】对话框

3）安全选项

安全选项用于设置对系统有安全威胁的策略的配置，例如是否允许匿名访问系统。安全选项内容比较多，这里介绍两个常用的配置，其他内容可以查看专业资料学习。

01 选择【安全设置】➢【本地策略】➢【安全选项】选项，右侧显示了所有的安全选项策略，如【网络访问：本地账户的共享和安全模型】，该选项可以设置本地共享的方式，双击该选项，如图 6-44 所示。

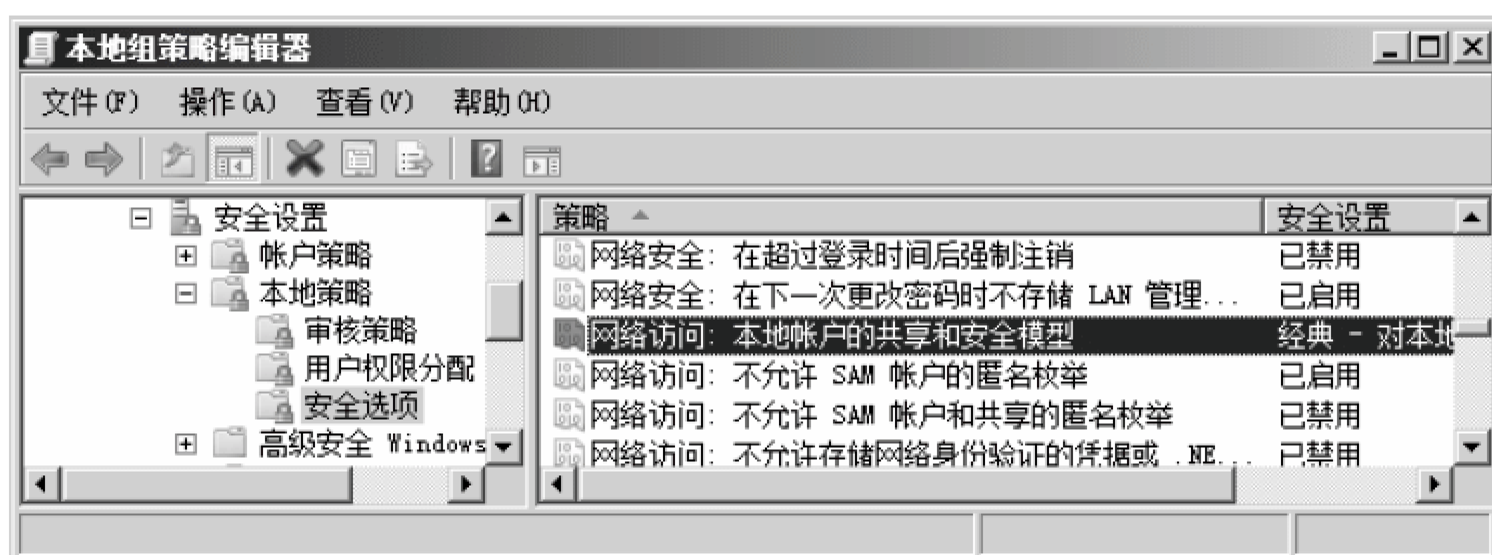


图 6-44 【安全选项】选项

02 弹出【网络访问：本地账户的共享和安全模型 属性】对话框，在【本地安全设置】选项卡中有一个下拉列表框，显示了两种本地共享模式：【经典】和【仅来宾】，一般采用“经典”模式，这样允许使用本地账户进行登录，如果采用“仅来宾”模式，则只允许使用来宾账户访问，如图 6-45 所示。

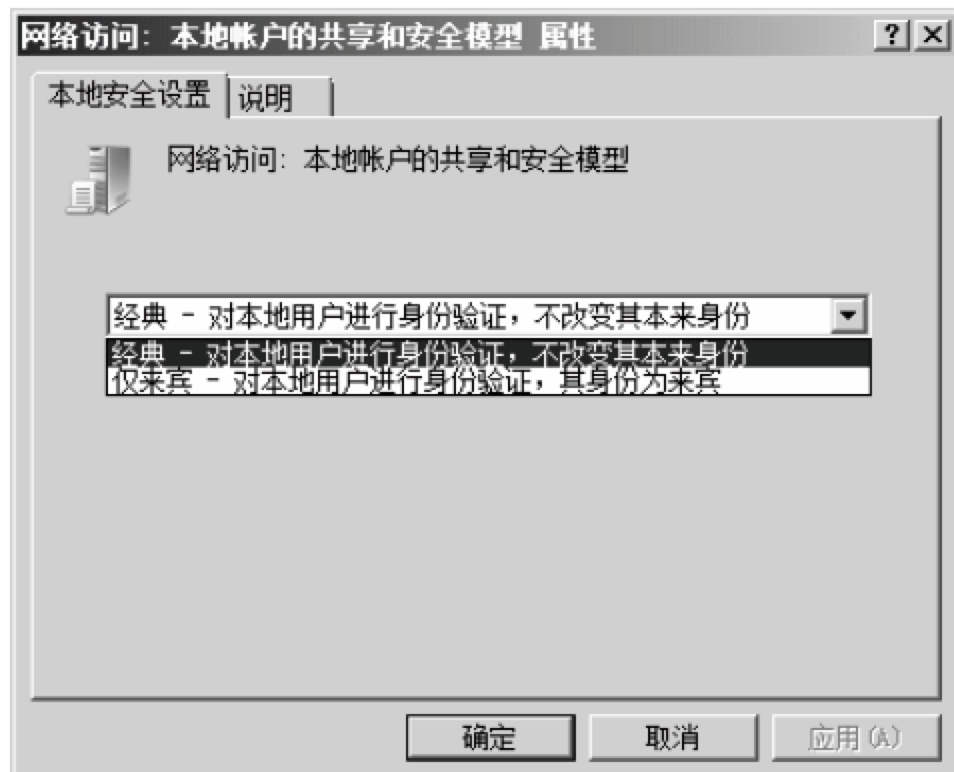


图 6-45 【网络访问：本地账户的共享和安全模型 属性】对话框

03 如果想完全禁止本地共享，在选择“仅来宾”共享模式的情况下，可以在安全选项下方找到【账户：来宾账户状态】选项，将来宾账户禁用，这样来宾账户不可用，就无法实现本地共享，如图 6-46 所示。

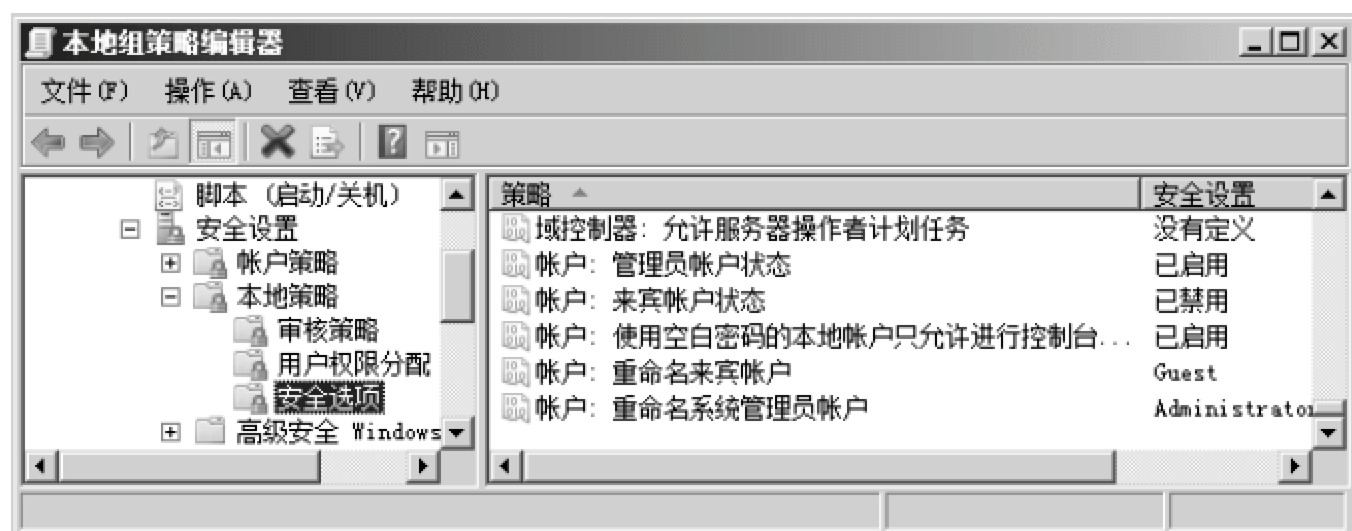


图 6-46　配置【账户：来宾账户状态】选项

6.3.4　项目实战 3：系统服务管理与系统瘦身

系统服务是系统运行中执行的服务项，例如系统运行网络功能就需要执行和网络相关的服务项。其实系统各种功能的体现很大一部分都是有对应的服务项负责的，合理维护系统服务项可以做到系统优化。下面简单介绍一下系统服务项的查看与管理。

01 选择【开始】➢【运行】选项，弹出【运行】对话框，在【打开】文本框中输入 “services.msc” 命令，单击【确定】按钮，如图 6-47 所示。



图 6-47　【运行】对话框

02 弹出【服务】窗口，窗口列表中显示了系统中所有的服务项，包括服务项名称、描述、启动状态和启动类型等内容，如图 6-48 所示。已启动的服务项越多，系统资源消耗越多。选择需要编辑的服务项，双击可以打开该服务项的属性对话框。

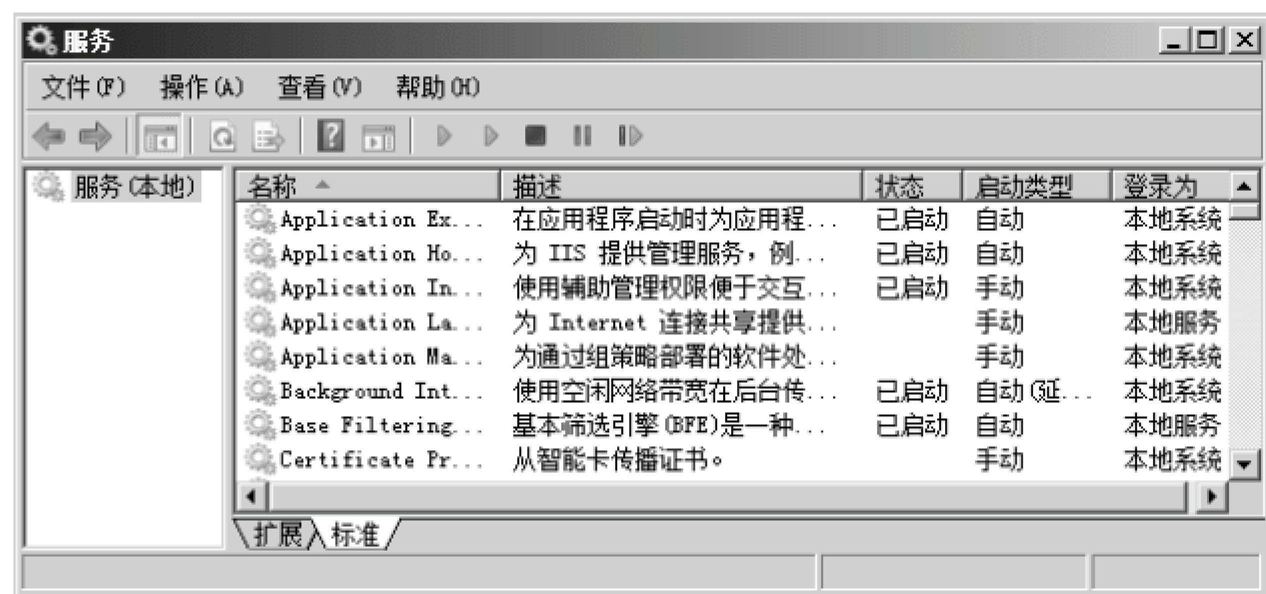


图 6-48　【服务】窗口

03 双击打开 DHCP Client 服务项，弹出属性对话框，在【启动类型】下拉列表中显示可用的启动类型，如果要将服务项永久关闭的话，可以选择【禁用】选项，然后单击【停止】按钮；如果临时停用该服务，直接单击【停止】按钮即可；如果需要服务根据需求自动启用，可以选择【自

动】选项；如果要手工确定其服务状态，则选择【手动】选项，并在【服务状态】区域单击需要的服务状态按钮。配置完成后单击【确定】按钮，如图 6-49 所示。

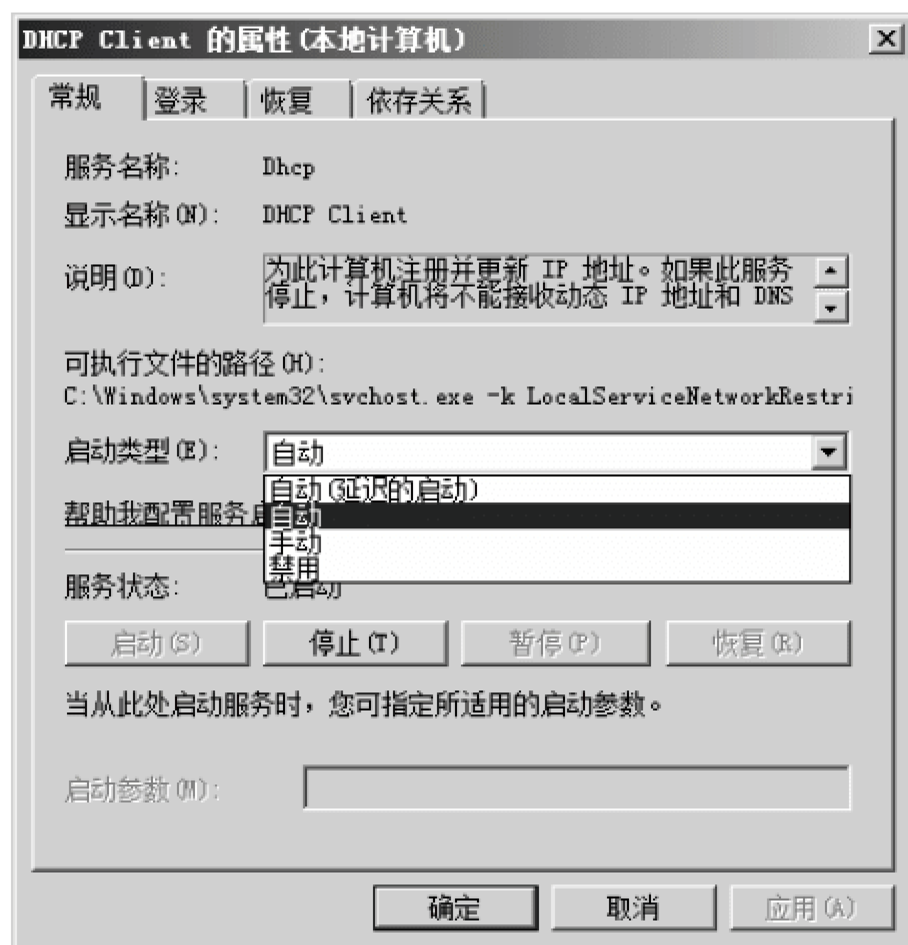


图 6-49　服务项属性对话框

读者可以查看每一个服务项的描述，或者查阅其他资料熟悉其功能，并根据需求将没有必要的服务项关闭，这样可以做到系统瘦身，提高系统性能、运行速度的作用。

除此之外，还有一些程序在删除时总是会有残余服务项无法清除，这些服务项会白白地浪费系统资源，读者应该在删除完软件程序后查看一下服务列表，确定将残留服务删除或禁用。

6.3.5　项目实战 4：利用系统开机启动项和进程发现计算机病毒和木马

计算机系统感染病毒和木马是常有的事，使用杀毒工具可以很轻松地将病毒和木马清除，但是有一些恶意的、较新的木马程序可能不那么容易清除，读者可以使用本节的内容轻松地发现这些病毒、木马，并将其清除。

1．利用系统开机启动项

系统开机运行时，总是有一些程序项目或服务会随机一起启动运行，大多数程序是为了提供更好的系统使用环境而设置的开机启动项，但是这一点往往会被计算机病毒或木马用于网络攻击。所以在系统中必须要将没有或者不认识的开机启动项删除。

一般可以使用专业的系统维护工具进行开机启动项检测和清除，也可以使用系统自带的工具进行操作，下面以系统自带程序演示清除系统开机启动木马的方法。

01　选择【开始】➢【运行】选项，弹出【运行】对话框，在【打开】文本框中输入“msconfig”命令，单击【确定】按钮，如图 6-50 所示。

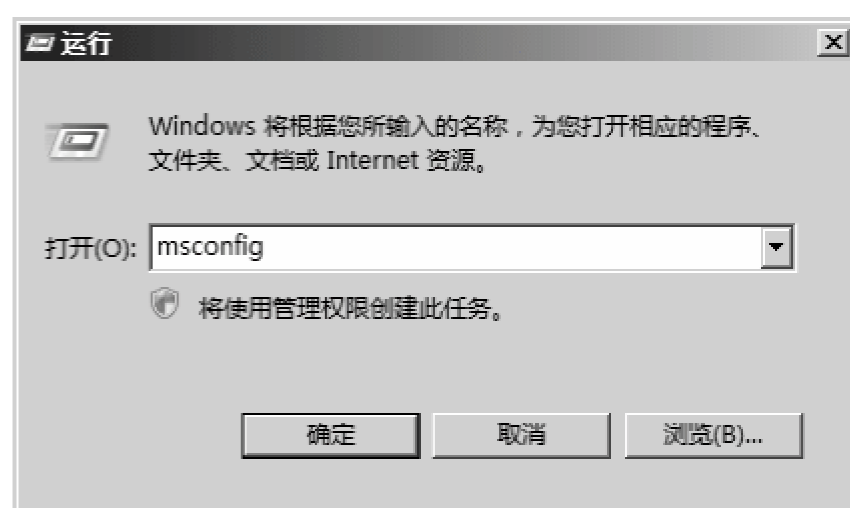


图 6-50　【运行】对话框

02 打开【系统配置】对话框，选择【启动】选项卡，在列表中显示了系统启动时随机启动的程序，其中第三项有“~”符号，第五项没有启动项目名，像这类有乱码或者没有名称的启动项都有可能是木马病毒，需要取消选中其复选框，如图 6-51 所示。



图 6-51　【系统配置】对话框

03 取消选中有安全威胁的系统启动项后，单击【确定】按钮，如图 6-52 所示。



图 6-52　取消选中有安全威胁的启动项

04 弹出【系统配置】提示框，系统重启后配置内容才会生效，单击【重新启动】按钮完成操作，如图 6-53 所示。

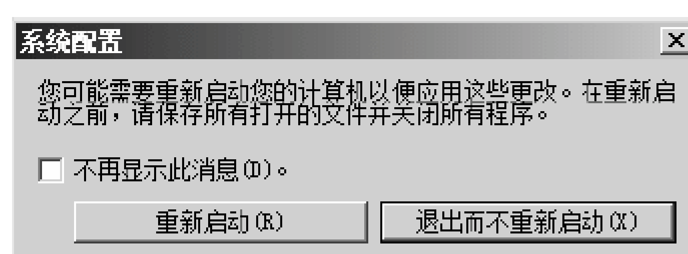


图 6-53　系统重启提示框

2. 使用系统进程

系统运行的任何一个程序都会在系统进程中体现出来，木马病毒一旦执行，同样也会在系统进程中显示出来。所以，读者发现系统异常时可以查看系统进程项，从中找出具有安全隐患的项目，将其手工关闭，具体操作方法如下。

01 可以通过【任务管理器】查看系统进程，具体操作方法可查看 6.3.1 节的内容，打开后如图 6-54 所示。读者应基本掌握常规进程的名称及意义，当发现不认识的进程或者有乱码的进程时，要及时利用互联网查询，看一看是否带有安全隐患，如果查询结果显示是木马程序，选中该项目，单击【结束进程】按钮将其关闭。

02 直接结束进程并不能将木马彻底删除，可以右击可疑的进程项，在弹出的快捷菜单中选择【打开文件位置】命令，找到该进程对应的执行文件位置，将其执行文件的相关内容直接删除能更好地清除安全威胁，如图 6-55 所示。



图 6-54 【任务管理器】对话框

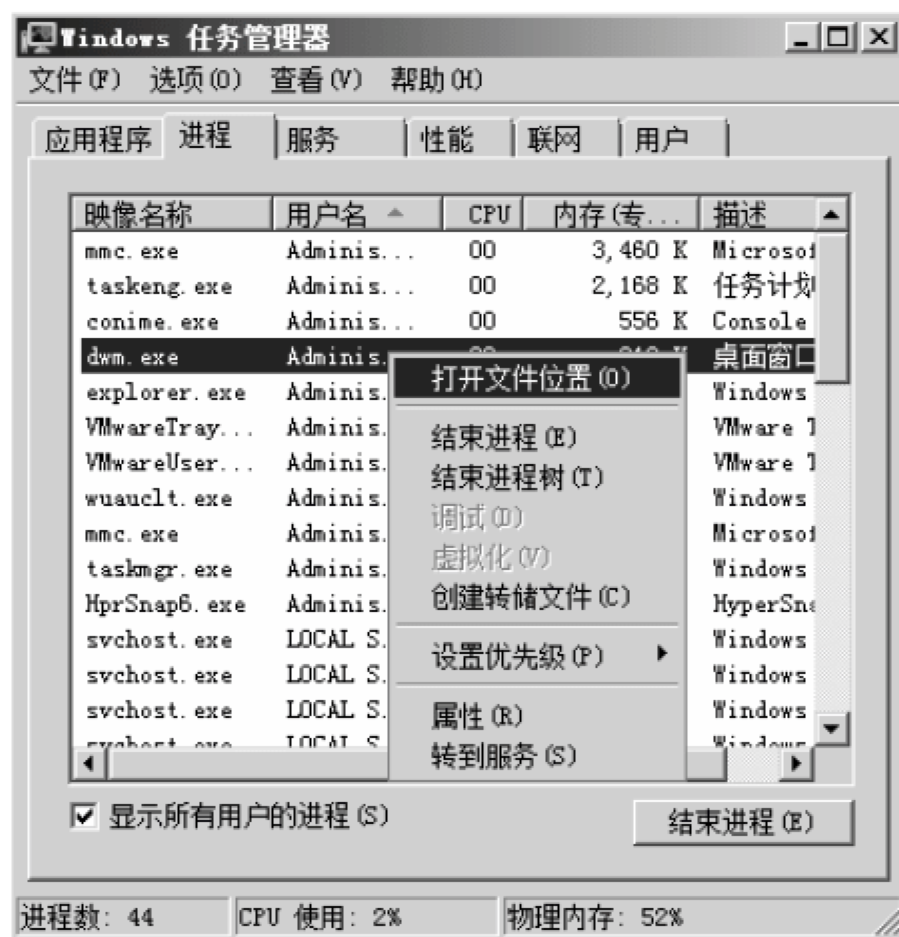


图 6-55 进程项的快捷菜单选项

6.4 DHCP 服务器的搭建与管理

DHCP 服务器是企业网络搭建中使用比较多的一种服务器类型。面对不断扩充的局域网用户数量，单靠人力手工配置 IP 地址根本无法满足需求，本节将详细介绍企业中 DHCP 服务器的应用。

6.4.1 架设 DHCP 服务器

DHCP 服务器是用来为其他主机自动分配 IP 地址的，其安装步骤如下：

01 选择【开始】➢【管理工具】➢【服务器管理器】菜单命令，弹出【服务器管理器】窗口，选择左侧【角色】选项，在右侧选择【添加角色】选项，如图 6-56 所示。



图 6-56 【服务器管理器】窗口

02 弹出【添加角色向导】对话框，如图 6-57 所示，单击【下一步】按钮。



图 6-57 【添加角色向导】对话框

03 弹出【添加服务器角色】对话框，如图 6-58 所示，选中【DHCP 服务器】复选框，单击【下一步】按钮。



图 6-58 【选择服务器角色】对话框

04 弹出【DHCP 服务器】对话框，显示了 DHCP 服务器的介绍，单击【下一步】按钮，如图 6-59 所示。

05 弹出【选择网络连接绑定】对话框，选择此 DHCP 服务器将用于向客户端提供服务的网络连接，本地只有一个网卡，选择后单击【下一步】按钮，如图 6-60 所示。

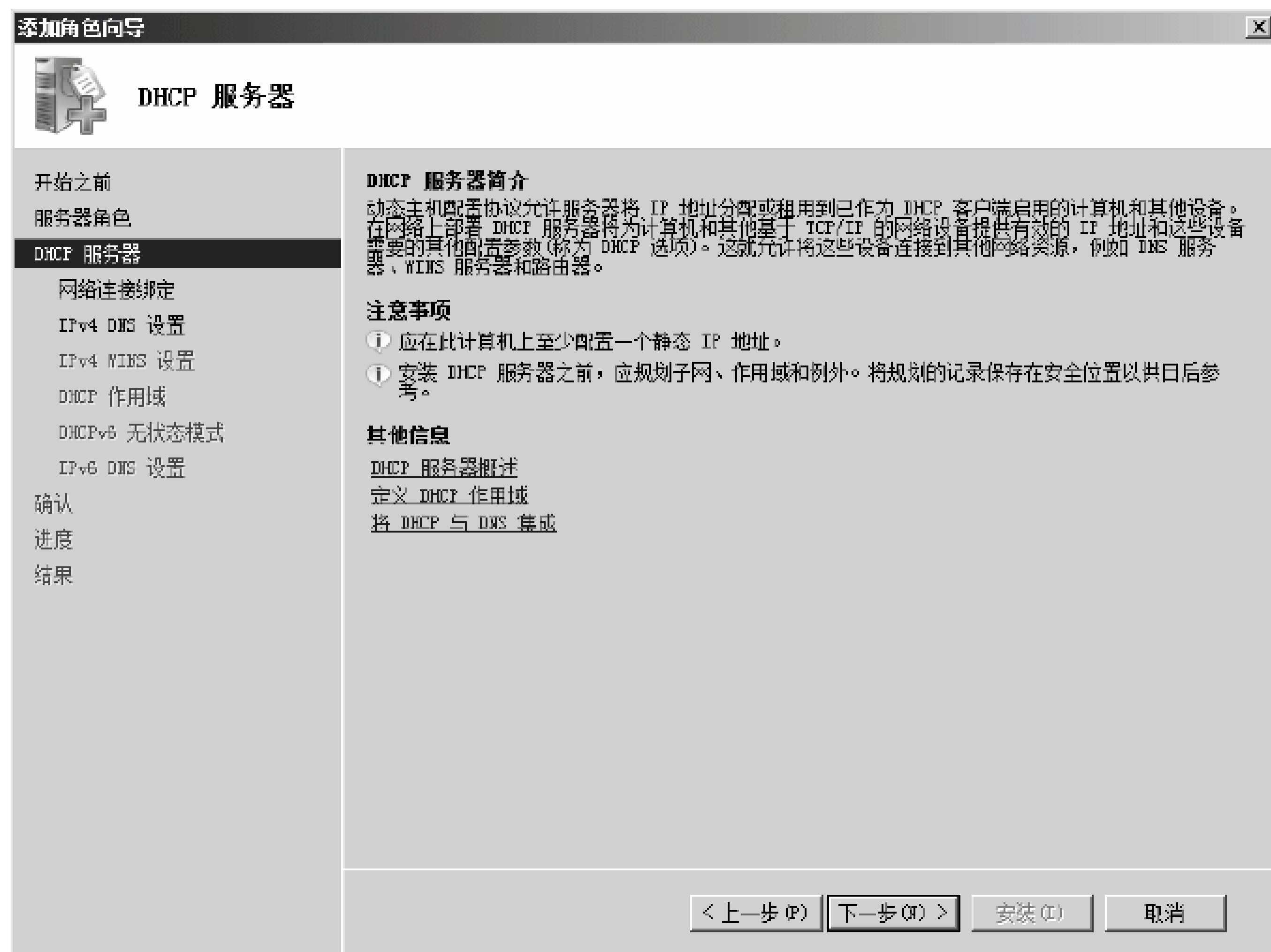


图 6-59 【DHCP 服务器】对话框

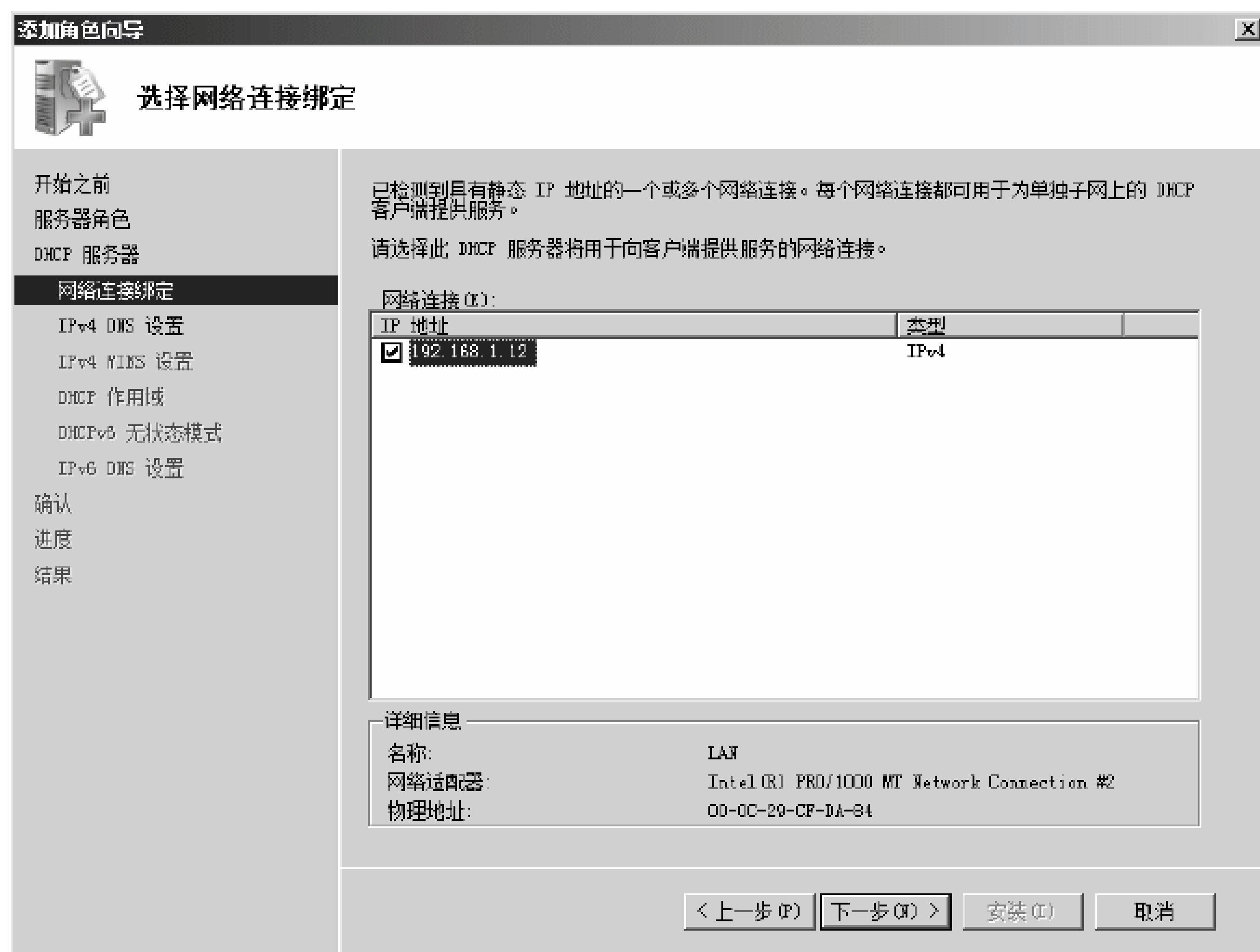


图 6-60 【选择网络连接绑定】对话框

06 弹出【指定 IPv4 DNS 服务器设置】对话框，设置 DHCP 服务器给客户端分配的 DNS 信息，暂不作配置，单击【下一步】按钮，如图 6-61 所示。

07 弹出【指定 IPv4 WINS 服务器设置】对话框，设置 DHCP 服务器给客户端分配的 WINS 信息，目前大部分网络已经不设置 WINS 服务器，选中【此网络上的应用程序不需要】复选框，单击【下一步】按钮，如图 6-62 所示。

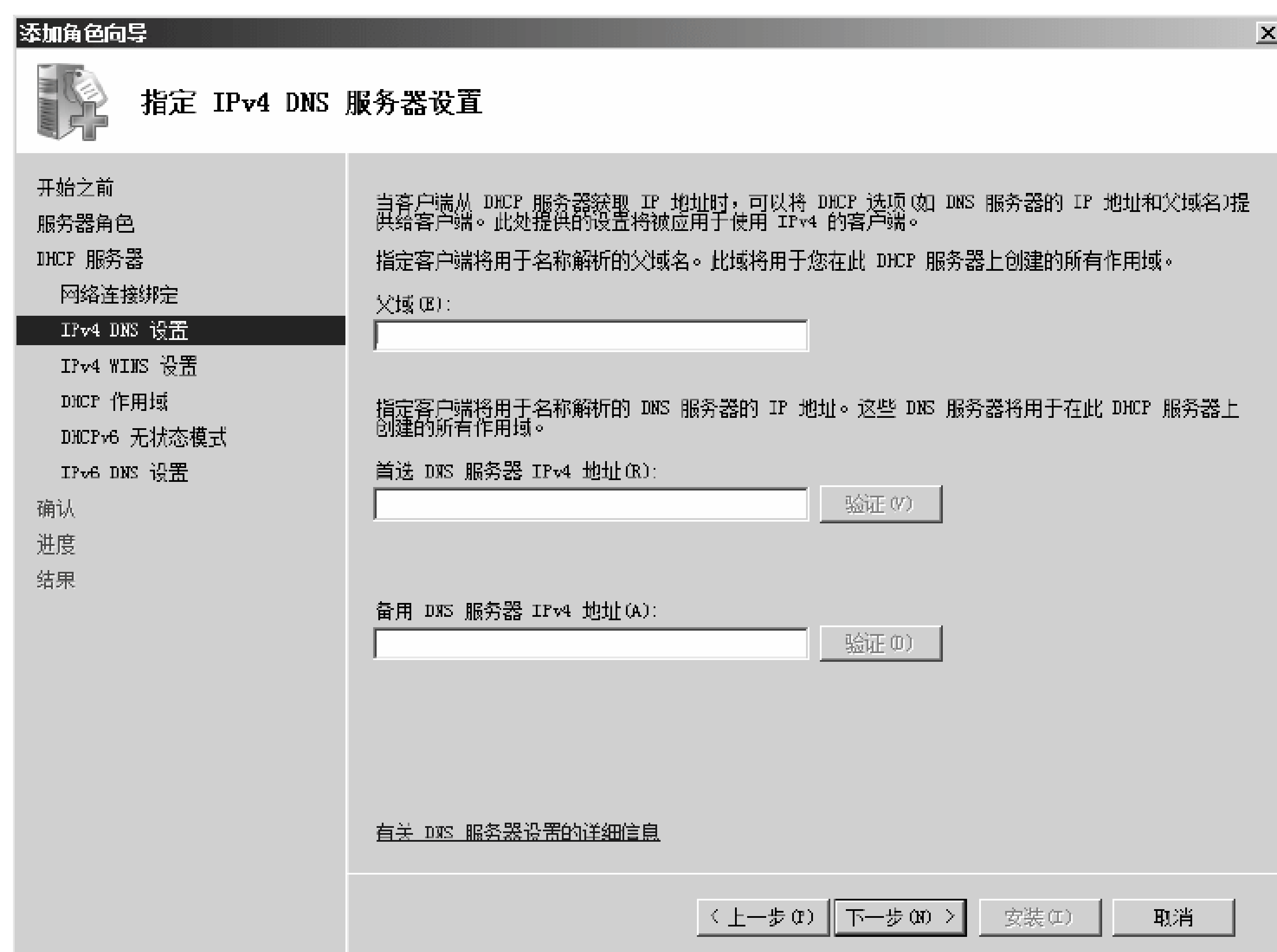


图 6-61　【指定 IPv4 DNS 服务器设置】对话框

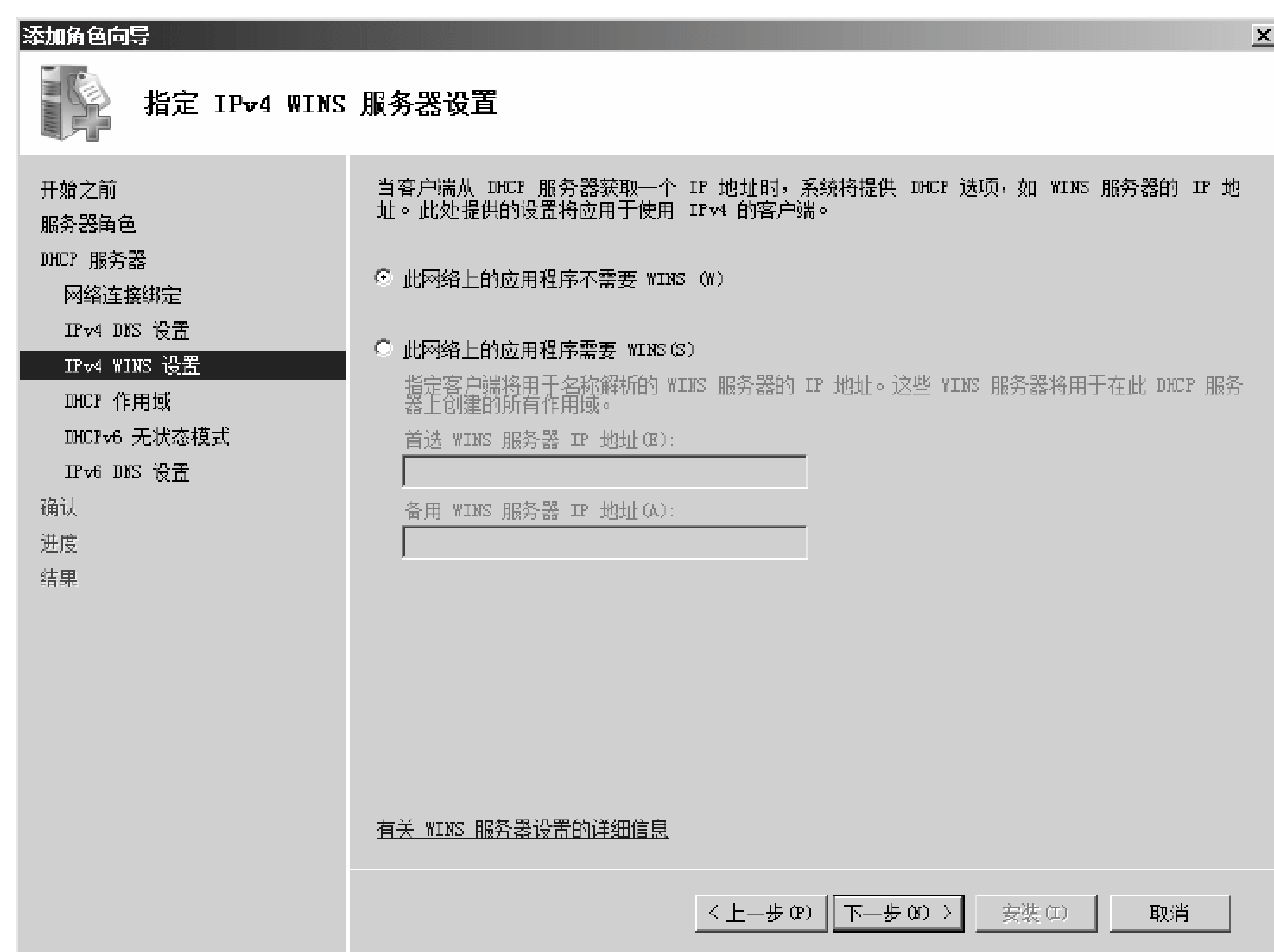


图 6-62　【指定 IPv4 WINS 服务器设置】对话框

08 弹出【添加或编辑 DHCP 作用域】对话框，暂不添加新作用域，单击【下一步】按钮，如图 6-63 所示。

09 弹出【配置 DHCPv6 无状态模式】对话框，如果网络中客户端自动配置 IPv6 地址，选中【对此服务器启用 DHCPv6 无状态模式】复选框，单击【下一步】按钮，如图 6-64 所示。

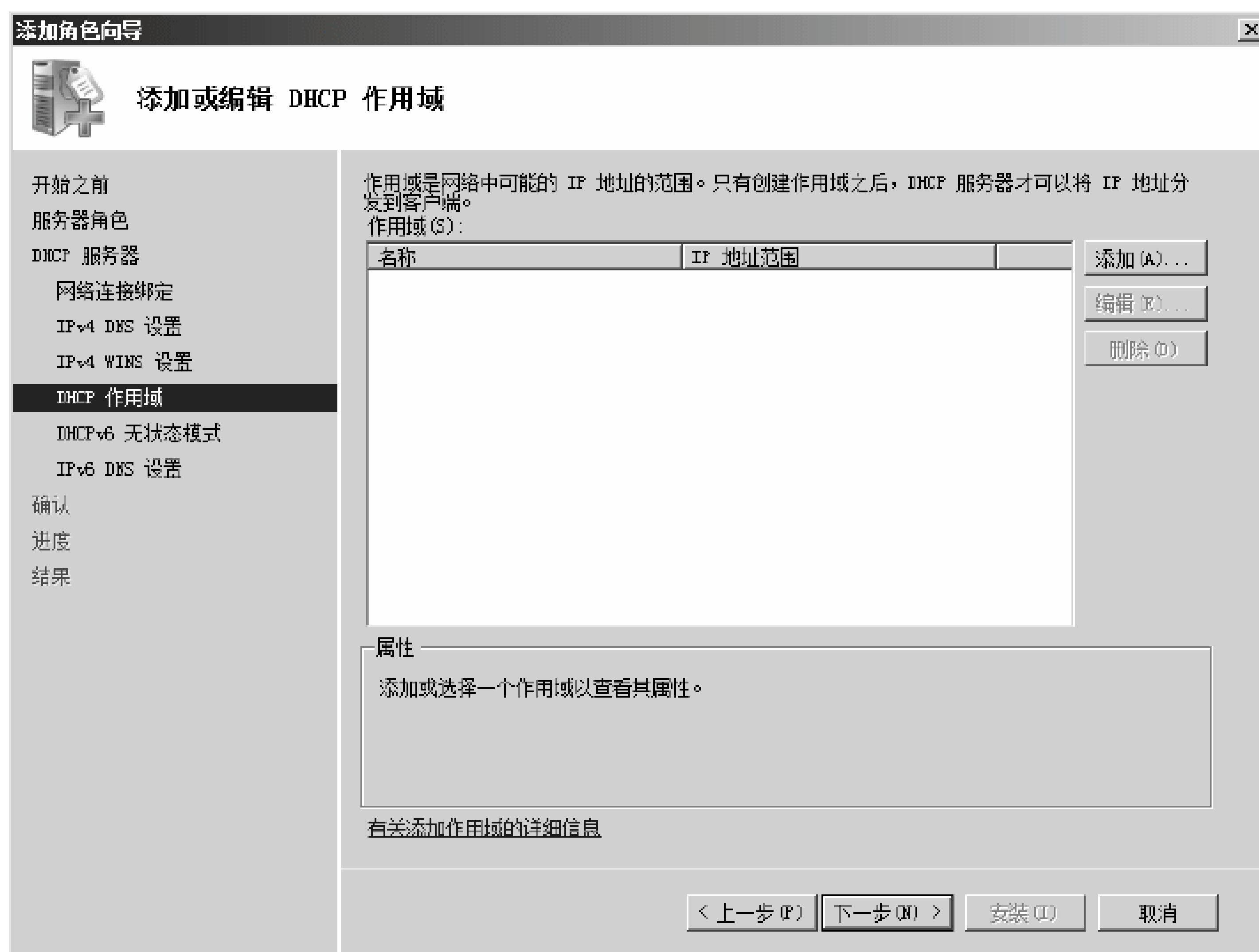


图 6-63 【添加或编辑 DHCP 作用域】对话框

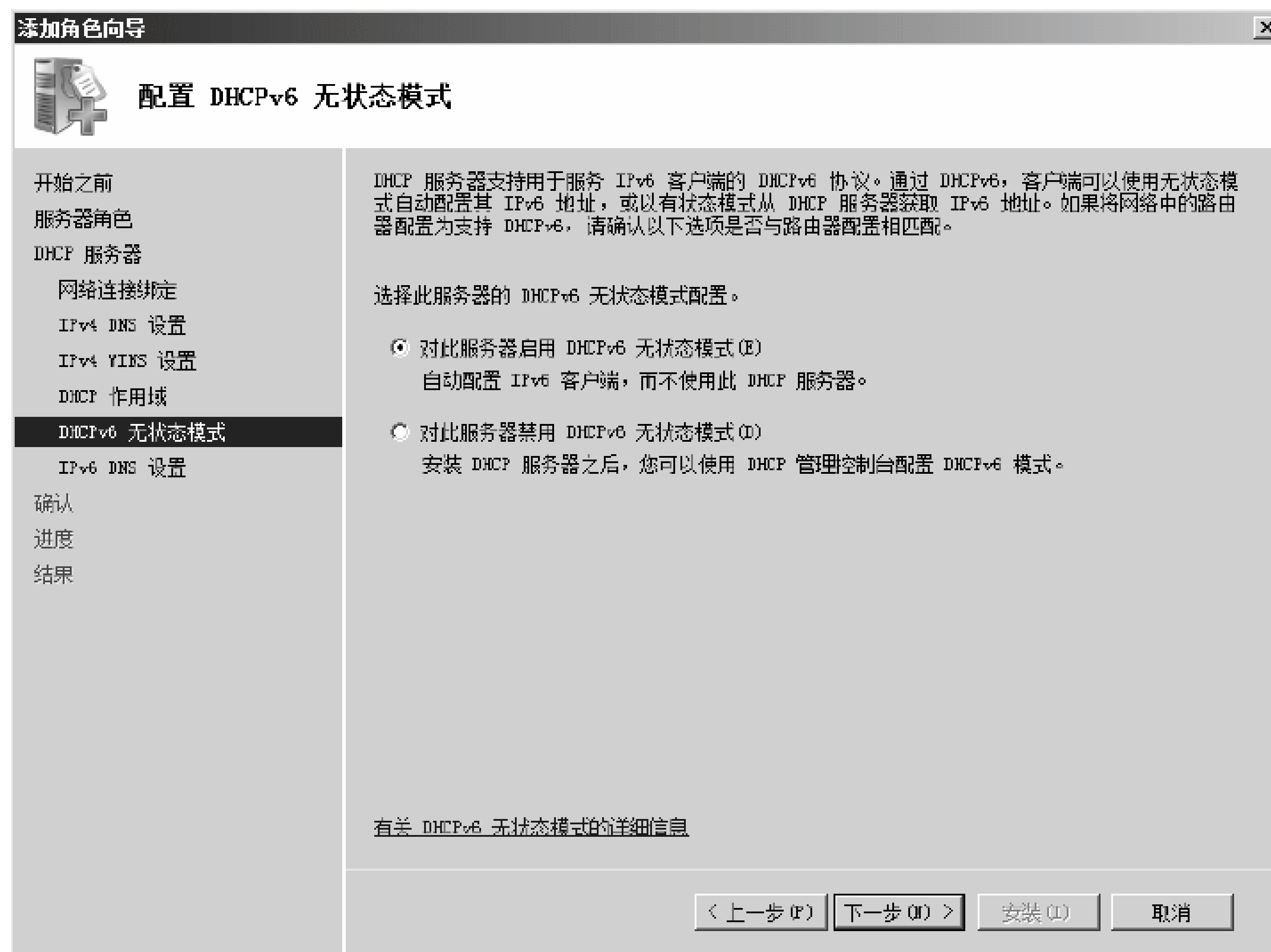


图 6-64 【配置 DHCPv6 无状态模式】对话框

10 弹出【指定 IPv6 DNS 服务器设置】对话框，为 IPv6 客户端设置 DNS 地址，本实例不作配置，单击【下一步】按钮，如图 6-65 所示。

11 弹出【确认安装选择】对话框，显示了安装 DHCP 的配置内容，单击【安装】按钮，如图 6-66 所示。

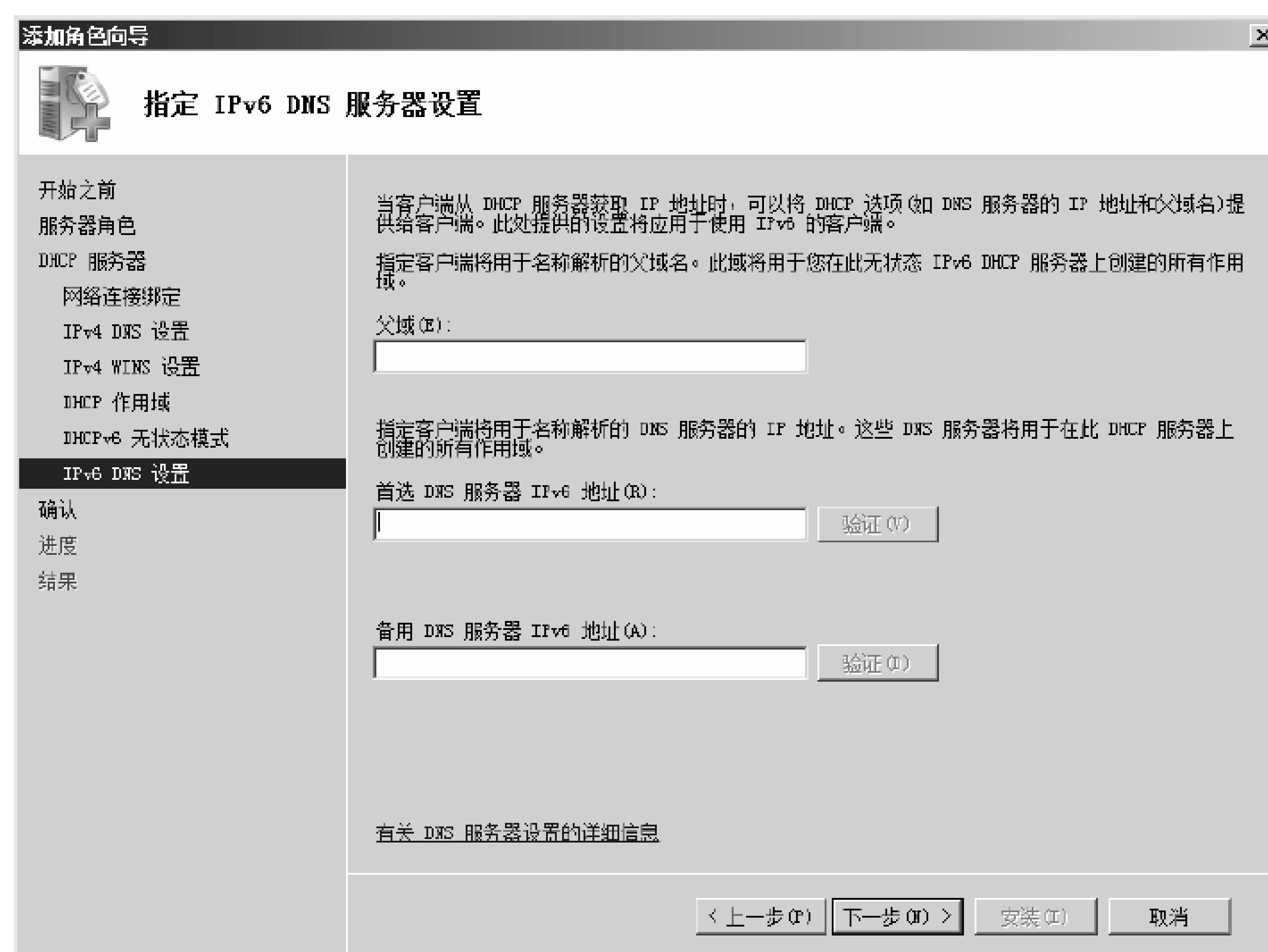


图 6-65 【指定 IPv6 DNS 服务器设置】对话框

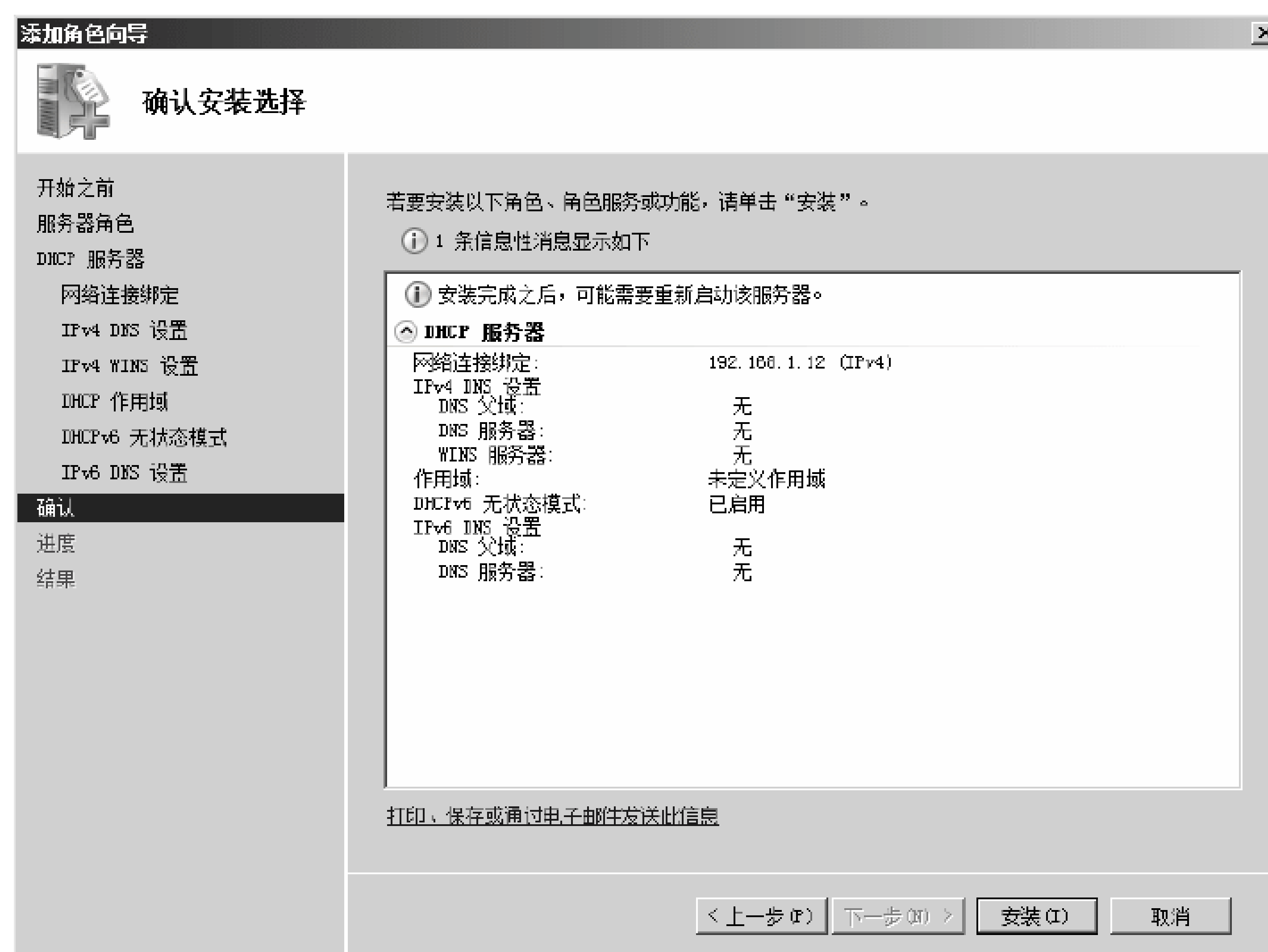


图 6-66 【确认安装选择】对话框

12 弹出【安装进度】对话框，开始安装 DHCP 服务，如图 6-67 所示。

13 安装完成，弹出【安装结果】对话框，显示 DHCP 服务安装成功，单击【关闭】按钮，如图 6-68 所示。



图 6-67 【安装进度】对话框



图 6-68 【安装结果】对话框

6.4.2 作用域的分配与创建

DHCP 服务器安装完成后要投入使用，需要为客户端配置可自动获得的地址范围，配置的地址范围可以用作用域来表示。作用域的具体创建方法如下。

01 选择【开始】➢【程序】➢【管理工具】➢【DHCP】命令，如图 6-69 所示。

02 弹出【DHCP】窗口，右击左侧选项中的【IPv4】选项，在弹出的快捷菜单中选择【新建作用域】菜单命令，如图 6-70 所示。



图 6-69 开始菜单选项

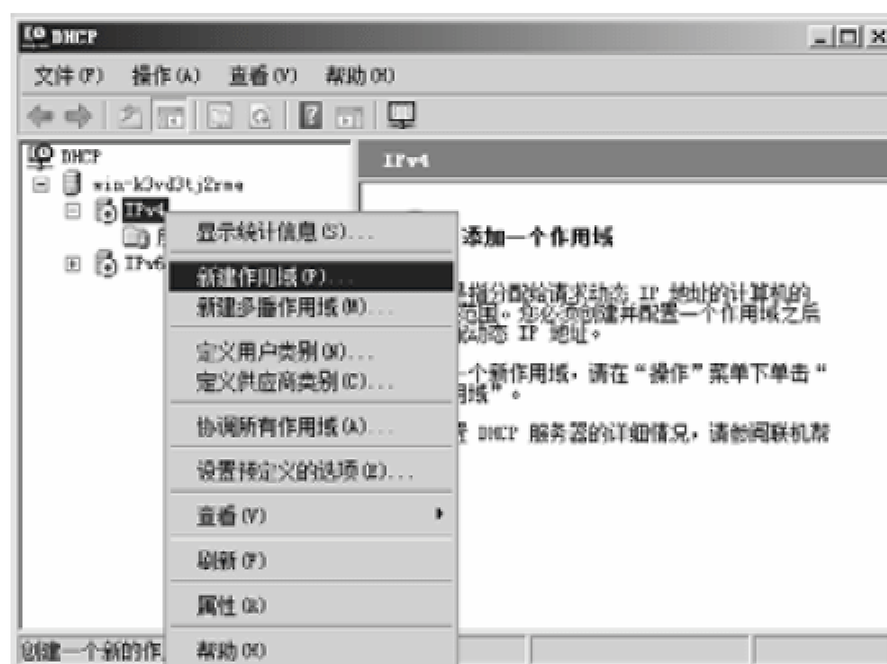


图 6-70 DHCP 窗口

03 弹出【新建作用域向导】对话框，单击【下一步】按钮，如图 6-71 所示。

04 弹出【作用域名称】对话框，在【名称】文本框中输入作用域的名称，本实例采用 network-1，单击【下一步】按钮，如图 6-72 所示。

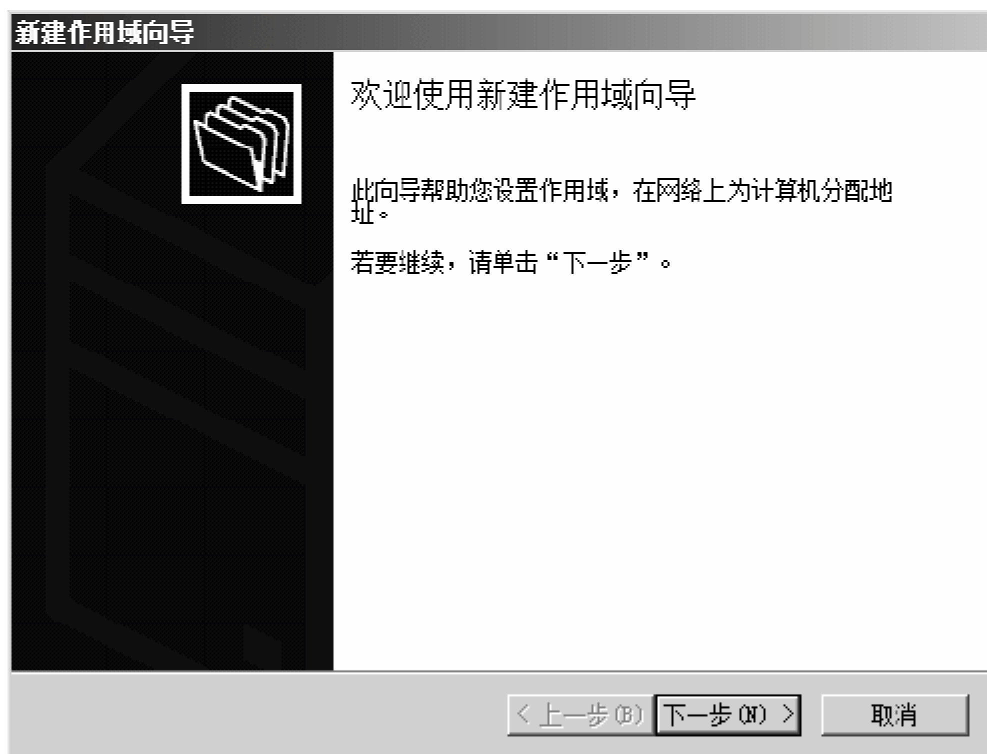


图 6-71 【新建作用域向导】对话框



图 6-72 【作用域名称】对话框

05 弹出【IP 地址范围】对话框，在【起始 IP 地址】和【结束 IP 地址】文本框中输入用于自动分配的地址区间，如图 6-73 所示，单击【下一步】按钮。

06 弹出【添加排除】对话框，在【起始 IP 地址】和【结束 IP 地址】文本框中输入 IP 地址范围中不用于自动分配的 IP 地址，一般为特定的服务器地址，本实例不配置，单击【下一步】按钮，如图 6-74 所示。

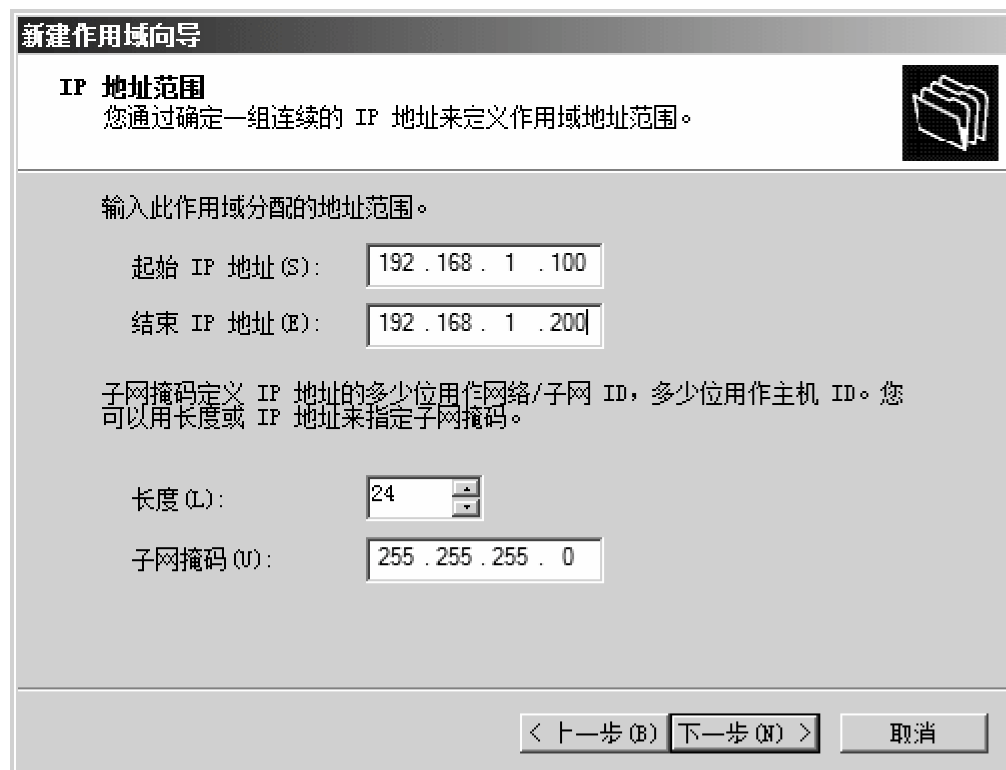


图 6-73 【IP 地址范围】对话框

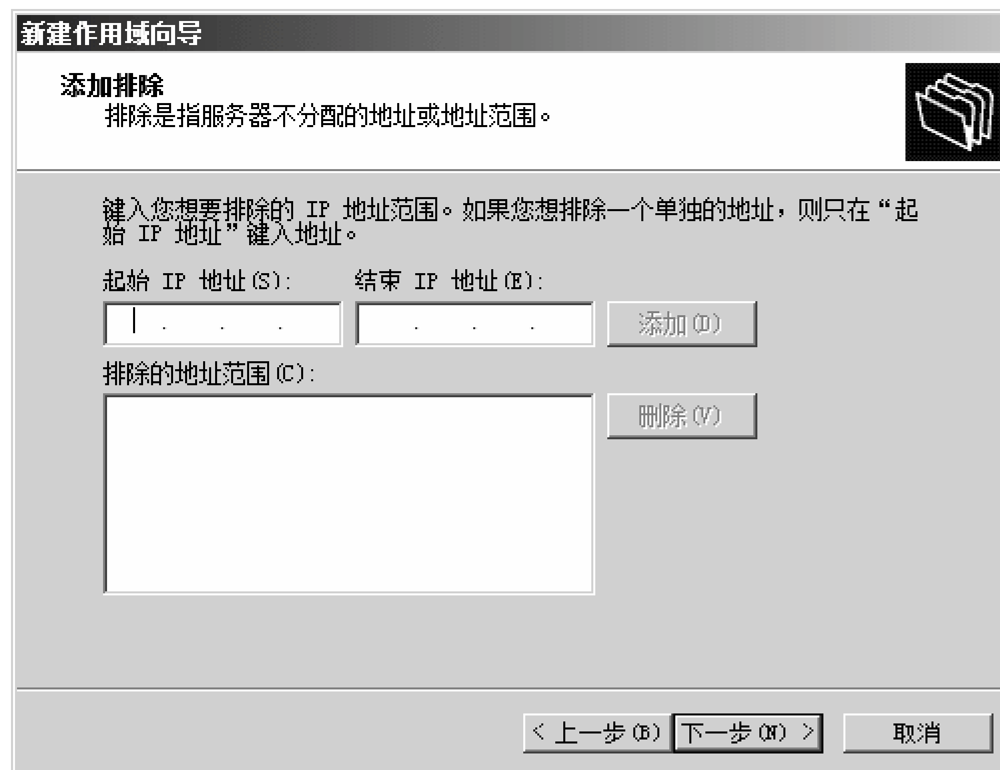


图 6-74 【添加排除】对话框

07 弹出【租用期限】对话框，默认 IP 地址的租约期限为“8”天，如果网络中以无限网络为主，为了安全，建议设置为6~8小时，单击【下一步】按钮，如图6-75所示。

08 弹出【配置 DHCP 选项】对话框，除了分配 IP 地址外，DHCP 服务器还可以附带其他选项一同分发，如默认网关（路由器）、DNS 服务器等，选中【是，我想现在配置这些选项】复选框，单击【下一步】按钮，如图6-76所示。

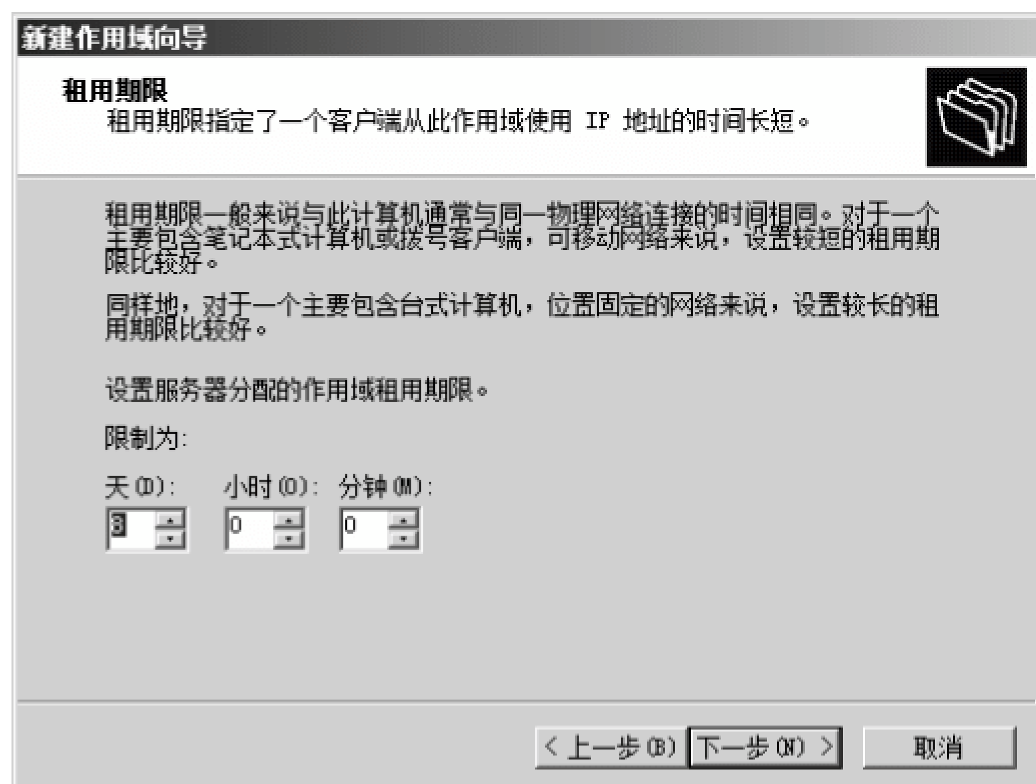


图 6-75 【租用期限】对话框

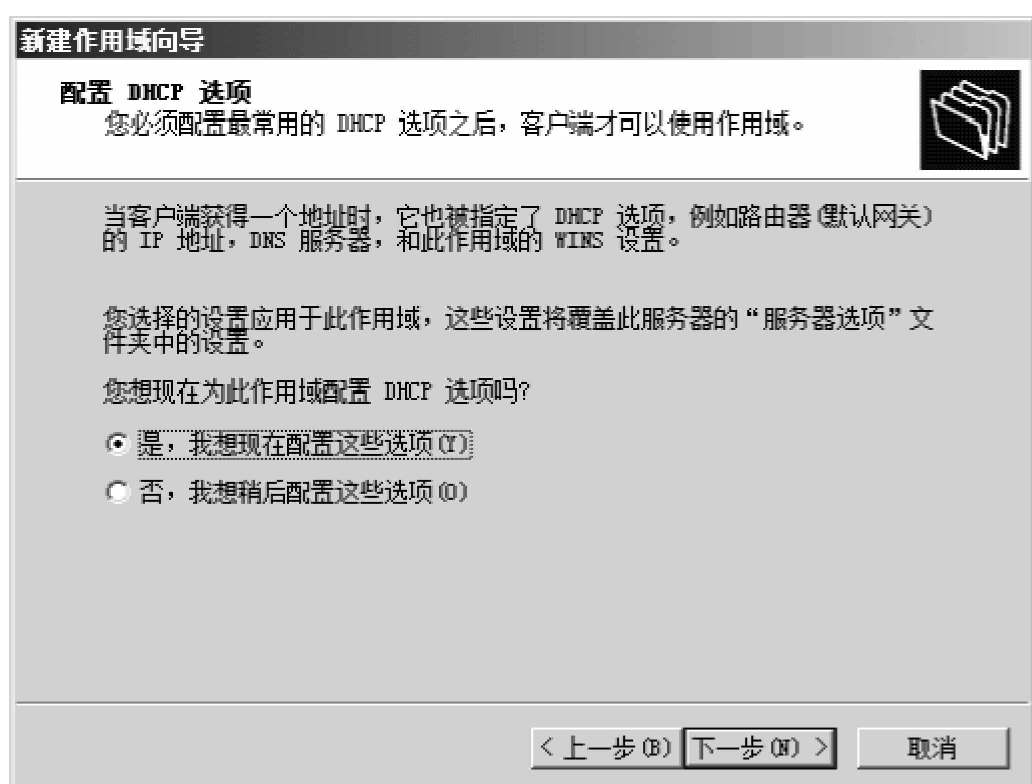


图 6-76 【配置 DHCP 选项】对话框

09 弹出【路由器（默认网关）】对话框，用于指定客户端的网关地址，是客户端访问外网必须要设置的内容，在【IP 地址】文本框中输入网关地址，本实例采用“192.168.1.1”，单击【添加】按钮，添加成功后单击【下一步】按钮，如图6-77所示。

10 弹出【域名称和 DNS 服务器】对话框，用于指定客户端进行域名解析需要的 DNS 服务器地址，直接在【IP 地址】文本框中输入有效的 DNS 服务器 IP 地址，单击【添加】按钮，添加成功后单击【下一步】按钮，如图6-78所示。

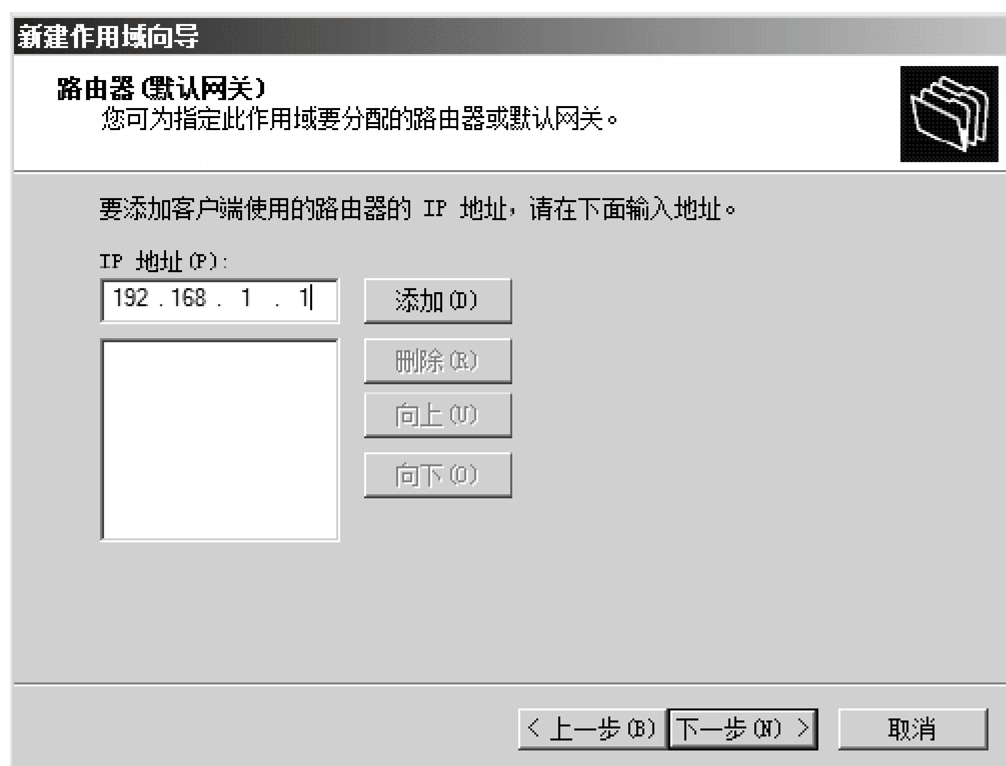


图 6-77 【路由器（默认网关）】对话框

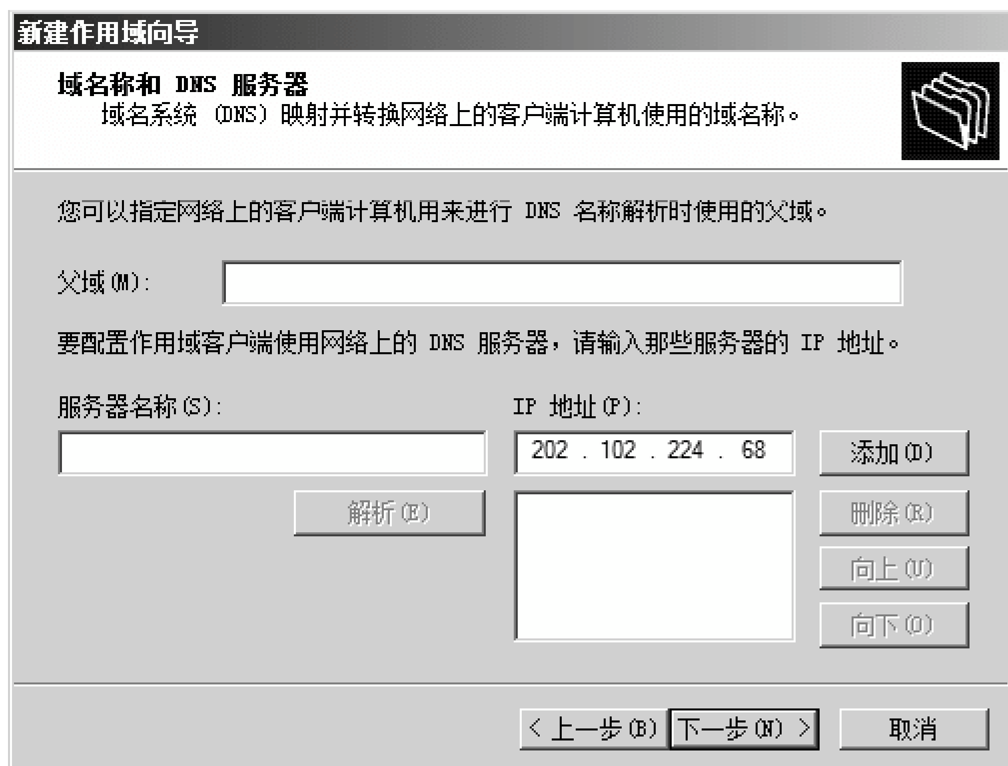


图 6-78 【域名称和 DNS 服务器】对话框

11 弹出【WINS 服务器】对话框，本实例不使用 WINS 服务器，单击【下一步】按钮，如图6-79所示。

12 弹出【激活作用域】对话框，选中【是，我想现在激活此作用域】复选框，单击【下一步】按钮，如图6-80所示。

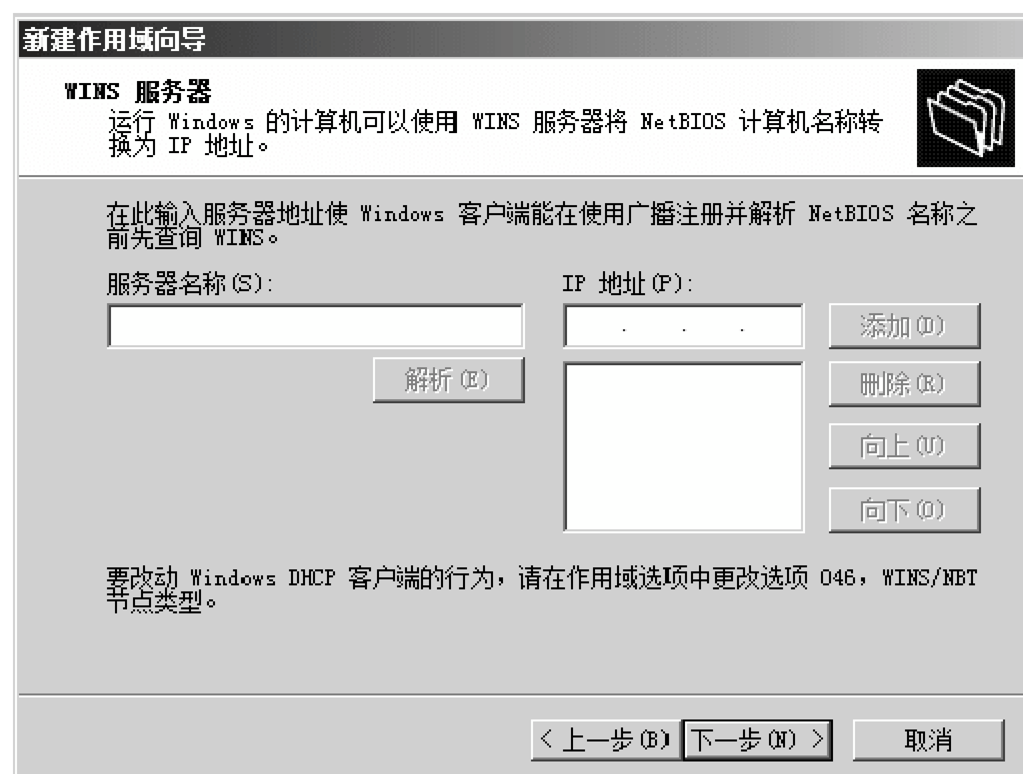


图 6-79　【WINS 服务器】对话框

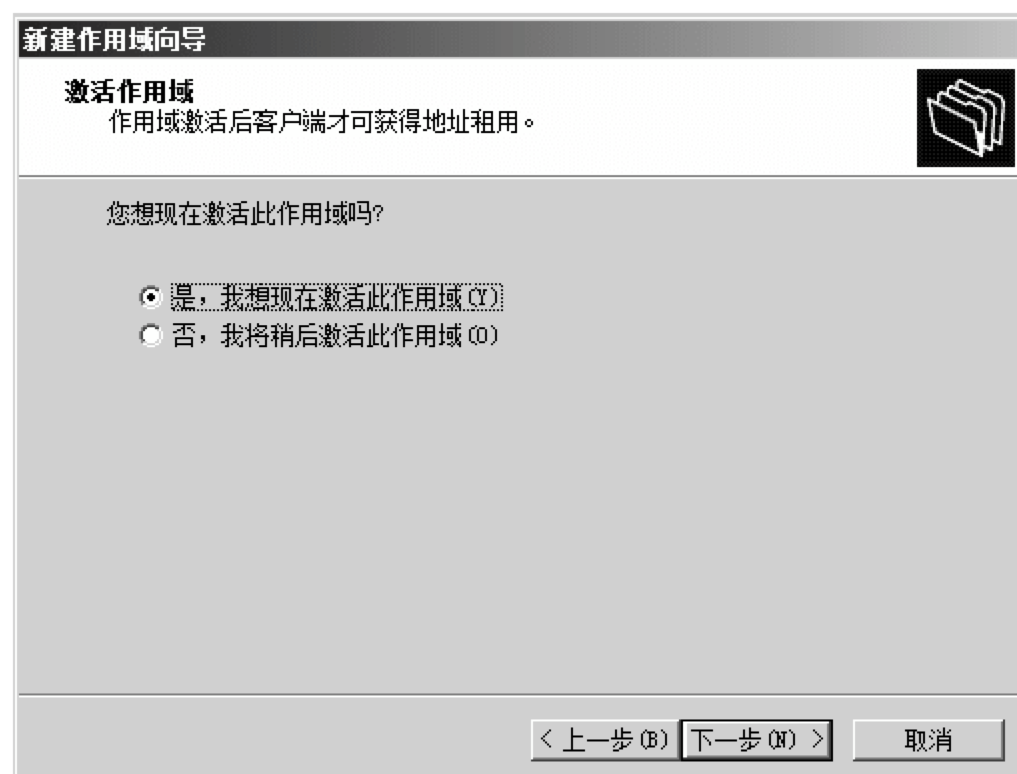


图 6-80　【激活作用域】对话框

13 弹出【正在完成新建作用域向导】对话框，单击【完成】按钮，结束新作用域添加向导，如图 6-81 所示。

14 返回【DHCP】窗口，新作用域添加成功，如图 6-82 所示。

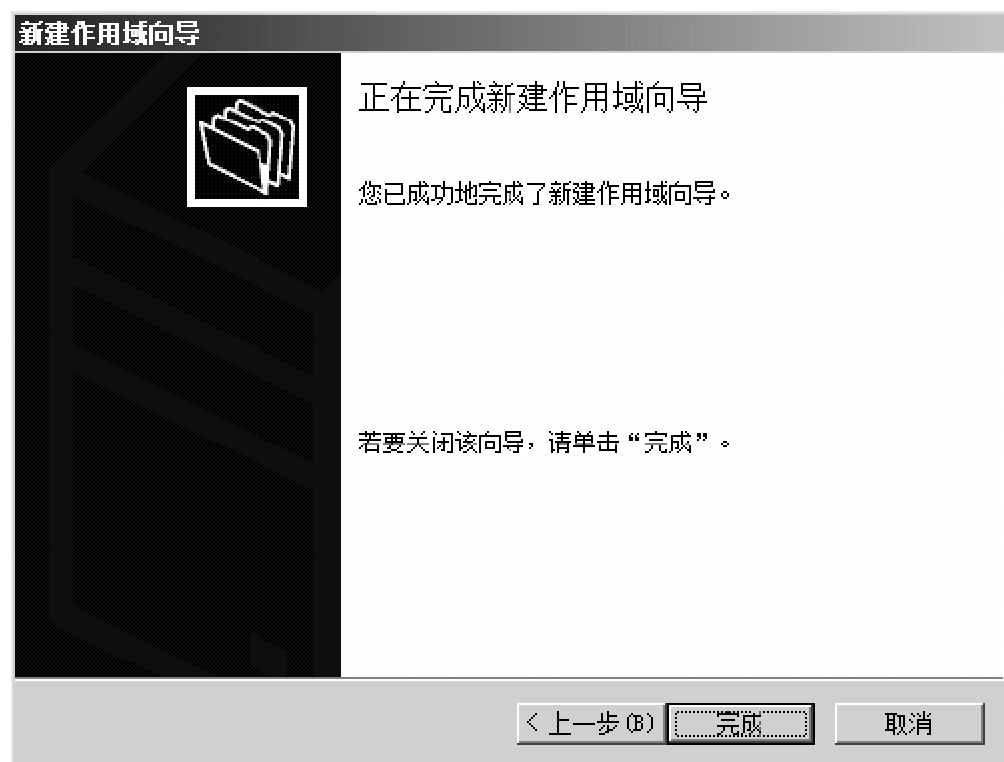


图 6-81　【正在完成新建作用域向导】对话框



图 6-82　【DHCP】窗口

在局域网中可能会使用 VLAN 技术配置有多个虚拟局域网，为了保证每一个 VLAN 的客户端都可以自动获得地址，要为每一个 VLAN 单独分配一个作用域，并分别对应 VLAN 的子网段。配置完成之后需要在局域网中负责多个 VLAN 虚拟局域网路由通信的核心设备配置 DHCP 中继，这里不作过多介绍。

需要注意的是，在一台主机配置多个网段的作用域时，每一个作用域的网段都必须在本地网卡配置，如果本地只有一个网卡，可通过以下方法为其配置多个网段的地址。

01 打开【本地连接 属性】对话框，选择【Internet 协议版本 4】选项，单击【属性】按钮，如图 6-83 所示。

02 弹出【Internet 协议版本 4（TCP/IP）属性】对话框，可以看到目前已经配置的 IP 地址，单击【高级】按钮，如图 6-84 所示。

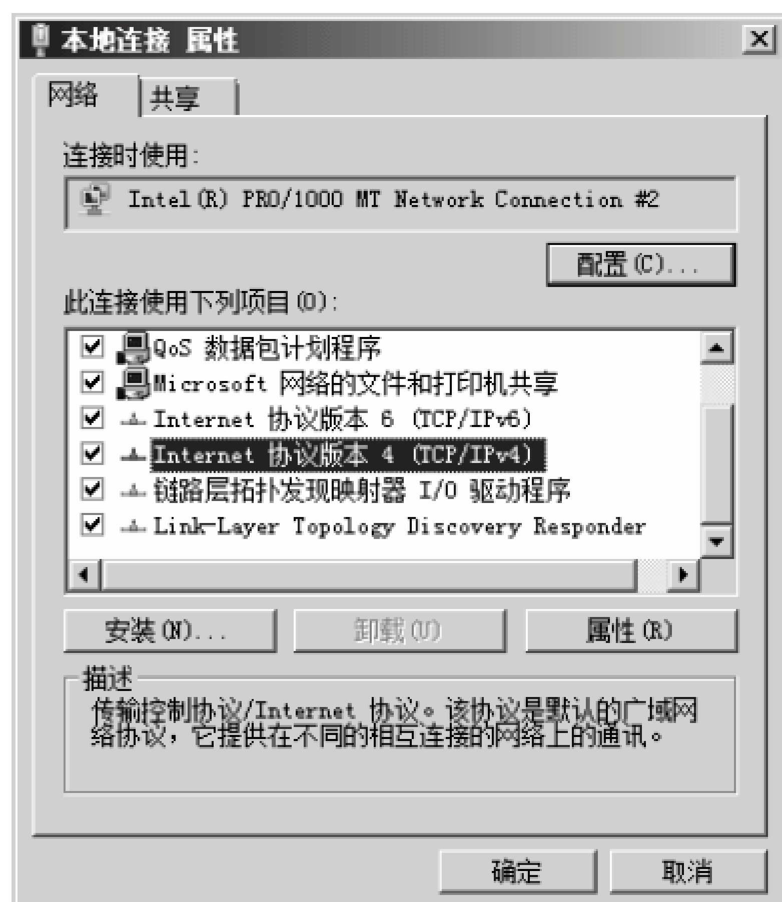


图 6-83 【本地连接 属性】对话框

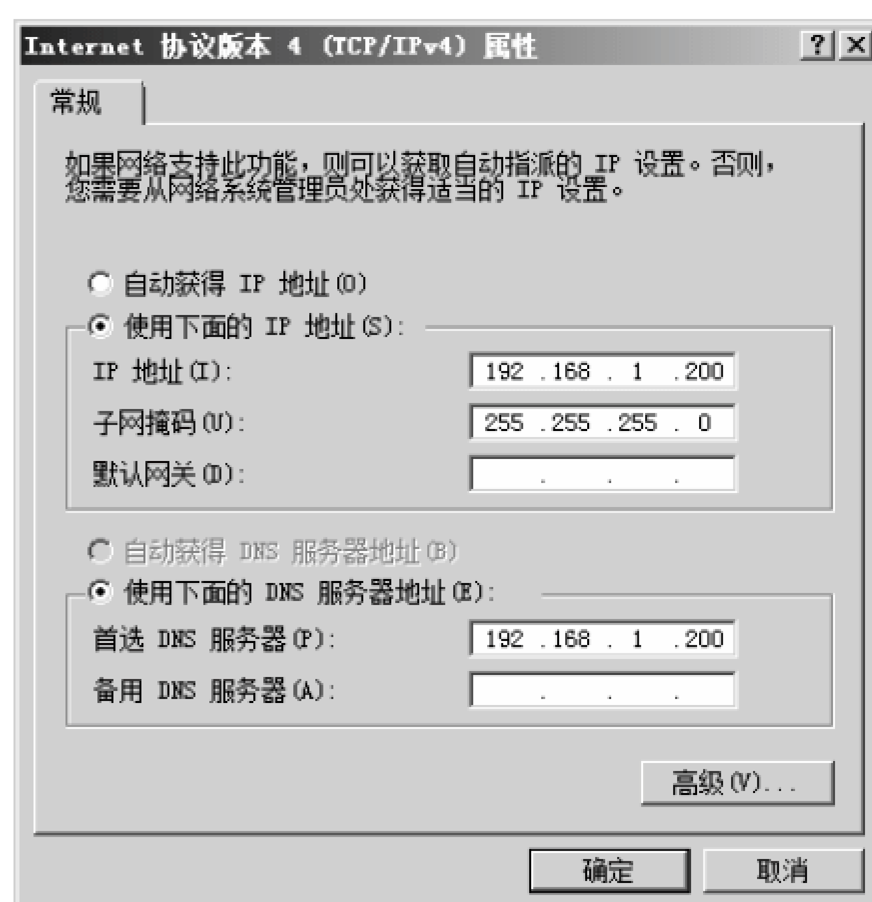


图 6-84 【Internet 协议版本 4（TCP/IPv4）属性】对话框

03 弹出【高级 TCP/IP 设置】对话框，选择【IP 设置】选项卡，在【IP 地址】区域中显示了已存在的 IP 地址，单击【添加】按钮可以增加新的 IP 地址，如图 6-85 所示。

04 弹出【TCP/IP 地址】对话框，填入新的网段的 IP 地址，如图 6-86 所示，单击【添加】按钮。



图 6-85 【高级 TCP/IP 设置】对话框



图 6-86 【TCP/IP 地址】对话框

05 返回【高级 TCP/IP 设置】对话框，在【IP 地址】区域中显示本地网卡存在有两个 IP 地址，且这两个 IP 地址属于两个网段，单击【确定】按钮完成配置，如图 6-87 所示。



图 6-87 【高级 TCP/IP 设置】对话框

6.4.3 为服务器配置保留地址

企业中用于提供关键服务的服务器设备一般不能随便更改其 IP 地址，所以在配置 DHCP 时，要针对这些服务器保留特定的 IP 地址，主要使用 IP 和 MAC 绑定的方式进行配置，具体操作步骤如下。

01 右击左侧列表中【作用域（192.168.1.0）network-1】作用域下的【保留】选项，在弹出的快捷菜单中选择【新建保留】菜单命令，如图 6-88 所示。

02 弹出【新建保留】对话框，在【保留名称】文本框中输入本次保留地址的名称，假设是为 server-1 服务器保留 IP 地址，输入“server-1”，在【IP 地址】文本框中输入需要保留的 IP 地址，在【MAC 地址】文本框中输入 server-1 服务器网卡的 MAC 地址，单击【添加】按钮，如图 6-89 所示。



图 6-88 DHCP 对话框

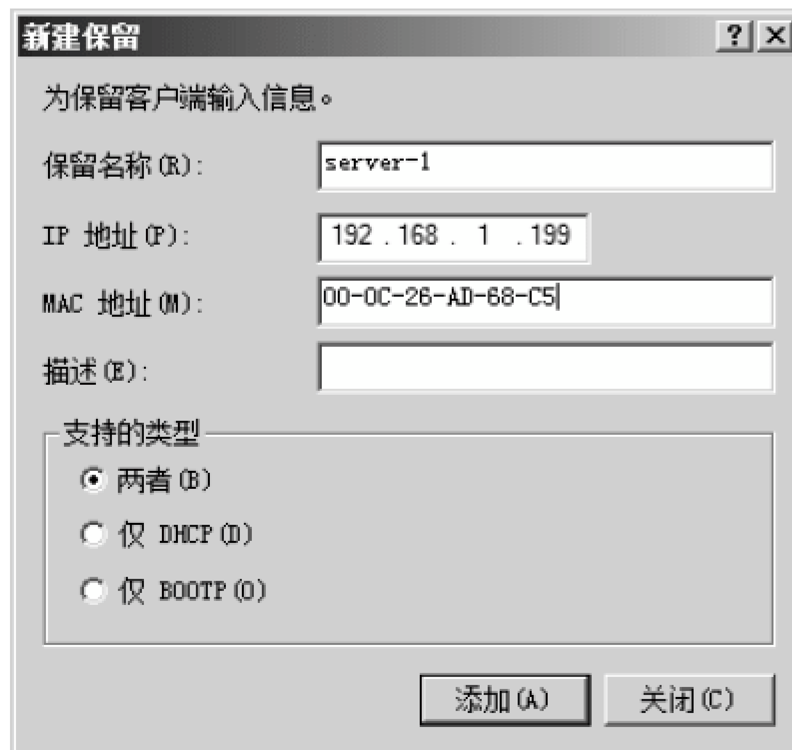


图 6-89 【新建保留】对话框



提 示

在【新建保留】对话框中输入的 MAC 地址用于识别服务器身份不能随意配置，而且 MAC 地址的输入格式要正确。

03 返回【DHCP】窗口，新建保留添加成功，新建保留地址可自动获得已配置的【路由器】和【DNS 服务器】信息，如图 6-90 所示。



图 6-90　保留地址配置成功

6.4.4　项目实战 5：备份与还原 DHCP 服务器的配置

随着局域网不断的扩充，DHCP 服务器管理分配的地址也越来越多，一旦服务器损坏，对网络的影响会很大。所以必须要对 DHCP 服务器的数据进行备份，当故障时可以使用备份数据迅速恢复。备份和还原 DHCP 服务器配置的操作方法如下。

1. 备份 DHCP 服务器的配置

备份 DHCP 服务器配置的具体操作步骤如下。

01 打开【DHCP】窗口，右击左侧选项列表中的服务器选项，在弹出的快捷菜单中选择【备份】命令，如图 6-91 所示。

02 弹出【浏览文件夹】对话框，选择备份文件存储的目录位置，默认为“C:\Windows\System32\dhcp\backup”目录，单击【确定】按钮，如图 6-92 所示。



图 6-91　DHCP 对话框



图 6-92　【浏览文件夹】对话框

2. 还原 DHCP 服务器的配置

当 DHCP 服务器发生故障之后，需要重新搭建 DHCP 服务器，将原来的配置备份文件直接恢复。

为了演示还原效果，可以将已存在的作用域全部删除，如图 6-93 所示，右击作用域选项，在弹出的快捷菜单中选择【删除】命令。



图 6-93　删除作用域

还原 DHCP 服务器配置的具体操作步骤如下。

01 打开【DHCP】窗口，右击左侧选项列表中的服务器选项，在弹出的快捷菜单中选择【还原】命令，如图 6-94 所示。

02 弹出【浏览文件夹】对话框，选择配置文件存放的目录位置，单击【确定】按钮，如图 6-95 所示。



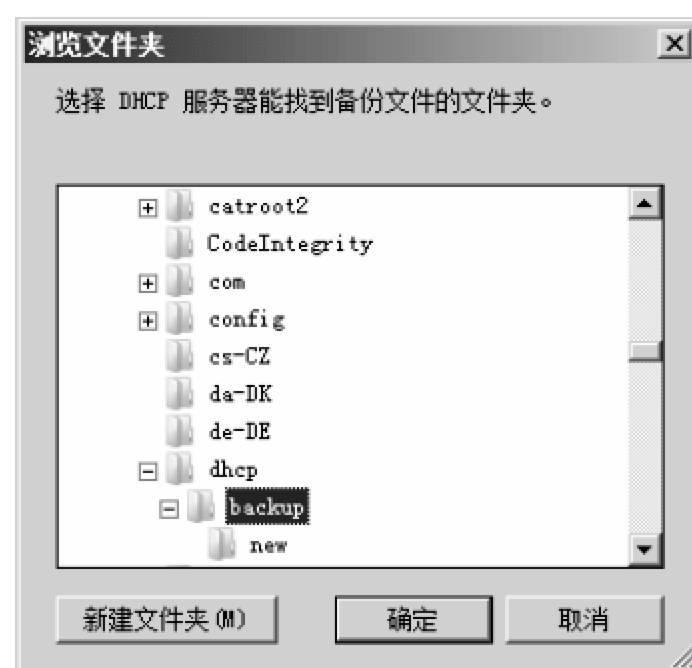
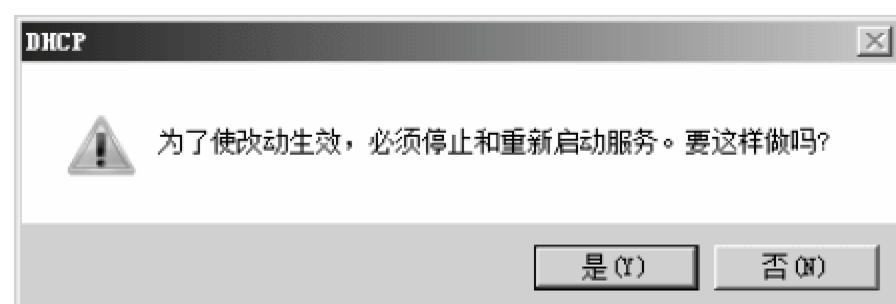


图 6-94　还原 DHCP 配置　　图 6-95　【浏览文件夹】对话框

03 弹出【DHCP】提示框，提示需要停止和重启 DHCP 服务使其生效，单击【是】按钮，如图 6-96 所示。

04 系统自动恢复配置文件，并重新启动 DHCP 服务器，如图 6-97 所示。



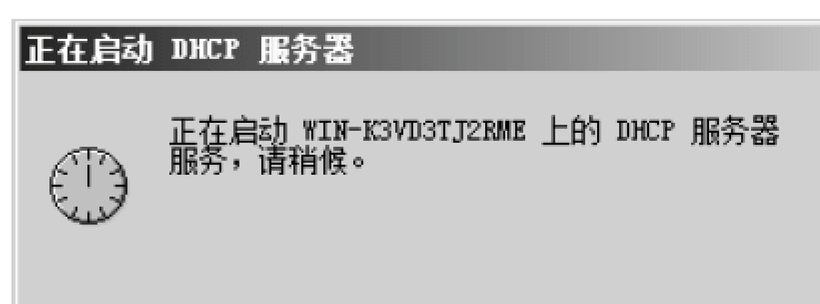


图 6-96　【DHCP】提示框　　图 6-97　启动 DHCP 服务器

05 还原成功后返回【DHCP】窗口，刚刚还原作用域并不能生效，显示有红色箭头，如图 6-98 所示。

06 刷新服务器，红色箭头变为绿色，DHCP 服务器正常使用，如图 6-99 所示。

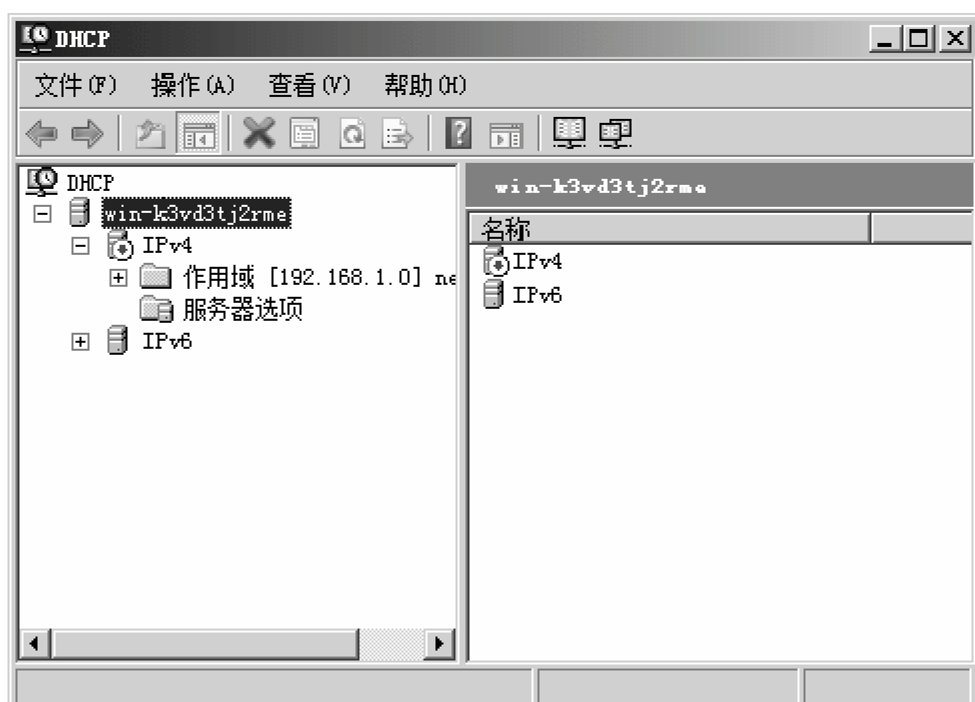


图 6-98 DHCP 还原成功



图 6-99 还原配置生效

6.4.5 项目实战 6：DHCP 服务器迁移

当需要更换服务器设备时，原有的 DHCP 服务器内容需要转移到新的服务器设备上，这时可以使用导入导出 DHCP 数据库的方式，实现 DHCP 服务器从一台服务器设备转移到另一台服务器设备。具体操作方法如下。

01 在已运行 DHCP 的服务器上选择【开始】➢【运行】选项，打开【运行】对话框，在【打开】文本框中输入“cmd”命令，单击【确定】按钮，如图 6-100 所示。

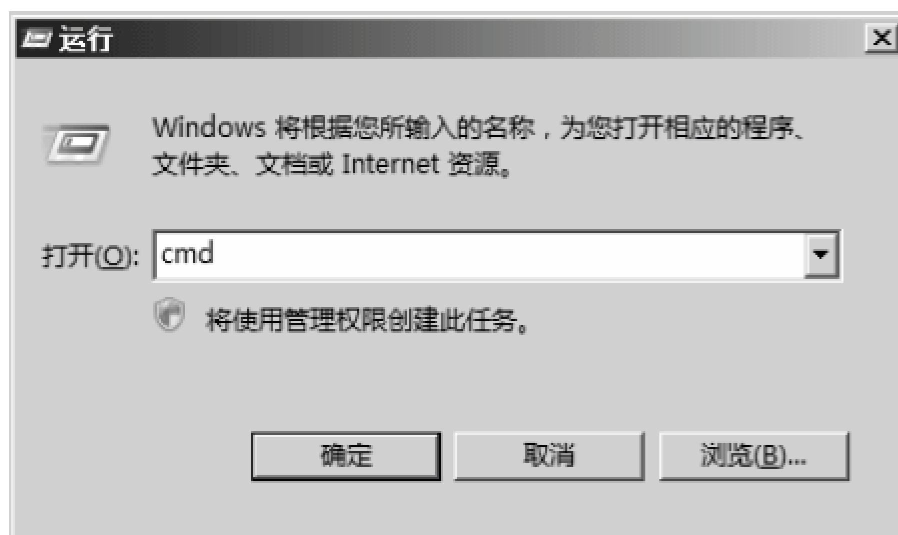


图 6-100 【运行】对话框

02 弹出命令行界面，直接输入“netsh dhcp server export c:\dhcpbackup.txt all”命令，按下 Enter 键，开始执行本服务器 DHCP 数据库的导出，导出目录位置及文件名为“c:\dhcpbackup.txt”，导出完成后如图 6-101 所示。



图 6-101 导出 DHCP 数据库

03 将导出的数据库文件 dhcpbackup.txt 拷贝到新服务器的磁盘上，选择存放在 C:\目录下。在新的服务器上安装 DHCP 服务，然后打开命令行界面，输入“netsh dhcp server import c:\dhcpbackup.txt all”命令，将拷贝的 DHCP 数据库文件导入本机中。如图 6-102 所示，数据库导入成功。



图 6-102　在新服务器上导入 DHCP 数据库


提　示

迁移操作时一定要使用系统管理员组的有效账户，如果新服务器要提升为域控制器，尽量先做迁移，后做域身份的升级。

6.5　打印服务器搭建与管理

打印服务器是企业办公环境中使用比较普遍的服务器，本节将详细介绍企业打印机的规划、选购，以及安装使用方法。

6.5.1　企业打印机的规划与采购

在规划企业打印机之前首先需要对企业打印服务进行分析，可以从以下几个方面考虑。

（1）打印速度：确定企业打印任务量，如果需要频繁打印大量文件，需要考虑选择打印速度快的打印机，打印速度一般安装每分钟的打印页数 ppm 进行描述。

（2）打印介质：包括普通纸张、卡片、信封等，这和企业业务需求有关。

（3）打印颜色：通常是黑白或者彩色，差不多的企业都会考虑彩色。

（4）打印机的数量和物理位置：这要考虑企业的实际业务量、建筑结构和网络布局。要尽量能够满足忙时打印任务的需求，同时打印机的物理分布要方便各个部门使用，方便安放、管理和维修等。

（5）打印权限：结合企业用户对打印机的使用权合理规划打印机权限配置，防止非法用户的使用。

通过对以上内容的分析基本上可以确定打印机的类型以及企业网络的业务需求，这样才能合理地规划打印服务器。下面简单介绍各种打印机的特征。

首先来介绍打印机的分类。打印机有多种分类方式，如接口类型、打印方式。按照打印方式一般可以分为喷墨打印机、激光打印机、针式打印机等，按照接口类型又可以分为网络打印机、USB 接口打印机、红外线接口打印机、连接到 LPT 端口或 COM 端口的打印机。

对按照打印方式分类的三种打印机进行简单比较，如表 6-2 所示。

表 6-2　三类打印机的优缺点

	优点	缺点	主要耗材	简介
针式打印机	可打印特殊介质，如复写纸	打印速度慢，噪音大	色带	主要应用在特殊行业和特殊设备中，如收款机、自动取款机
喷墨打印机	价格便宜，可打印黑白和彩色	打印速度较慢，墨盒耗材成本较高	墨盒	主要应用于家庭，彩色的喷墨打印机可以用于打印照片、彩色图纸等
激光打印机	打印速度快，打印效果很好，打印平均成本低	价格昂贵	硒鼓	是公司中使用最广泛的文件打印机

接口类型对打印机的选购影响并不是很大，只要接口能连接使用就可以。

剩下的就是品牌选择，目前存在的打印机品牌比较多，如惠普、佳能、三星、联想、富士施乐、爱普生、方正和戴尔等。每一个品牌都有自己的特征，读者可以结合对这些品牌的喜好和价格进行选择。

6.5.2　项目实战 7：安装企业打印机

使用打印机时，并非直接连接就可以使用，需要使用专门的打印机管理服务器进行操作，下面详细介绍打印机的安装配置方法。

1. 安装打印服务器

首先需要安装打印机管理服务器，具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，在左侧选择【角色】选项，在右侧选择【添加角色】选项，如图 6-103 所示。



图 6-103　【服务器管理器】窗口

02 弹出【添加角色向导】对话框，如图 10-104 所示，单击【下一步】按钮。

03 弹出【添加服务器角色】对话框，如图 10-105 所示，选中【打印服务】复选框，单击【下一步】按钮。



图 6-104　【添加角色向导】对话框

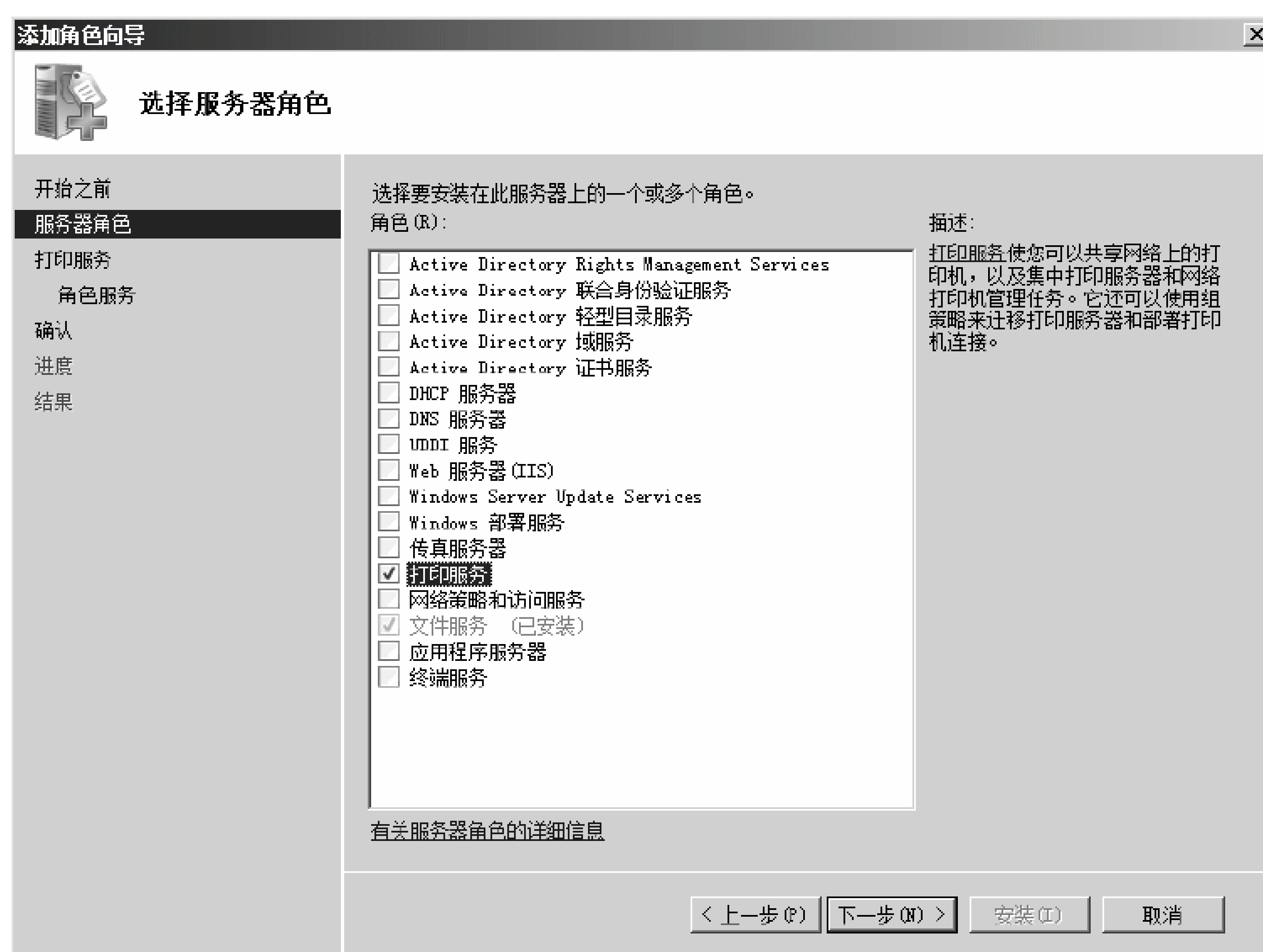


图 6-105　【添加服务器角色】对话框

04 弹出【打印服务】对话框，显示打印服务的简介信息，单击【下一步】按钮，如图 6-106 所示。

05 弹出【选择角色服务】对话框，选择打印服务需要安装的角色内容，默认只选中了【打印服务器】复选框，为了方便管理员使用 Web 界面管理打印服务器，建议选中【Internet 打印】复选框，如图 6-107 所示。



图 6-106 【打印服务】对话框



图 6-107 【选择角色服务】对话框

06 选中【Internet 打印】复选框后，弹出【添加角色向导】对话框，显示需要安装的 Web 服务内容，单击【添加必需的角色服务】按钮，如图 6-108 所示。

07 返回【选择角色服务】对话框，单击【下一步】按钮，如图 6-109 所示。

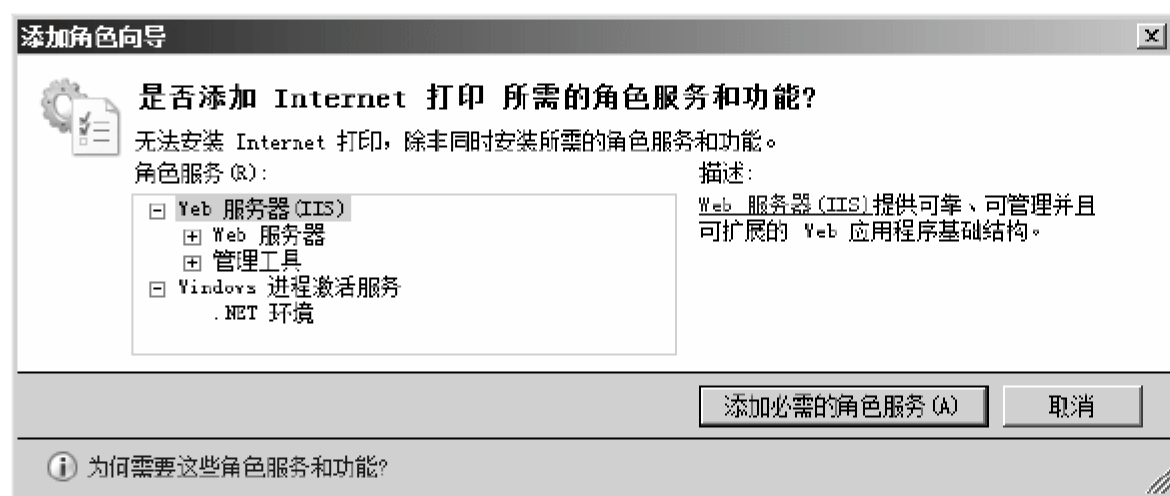


图 6-108 【添加角色向导】对话框



图 6-109　【选择角色服务】对话框

08 弹出【Web 服务器（IIS）】对话框，显示 Web 服务器简介，单击【下一步】按钮，如图 6-110 所示。

09 弹出【选择角色服务】对话框，显示 Web 服务器角色列表，选择需要安装的组件，本实例采用默认配置，单击【下一步】按钮，如图 6-111 所示。

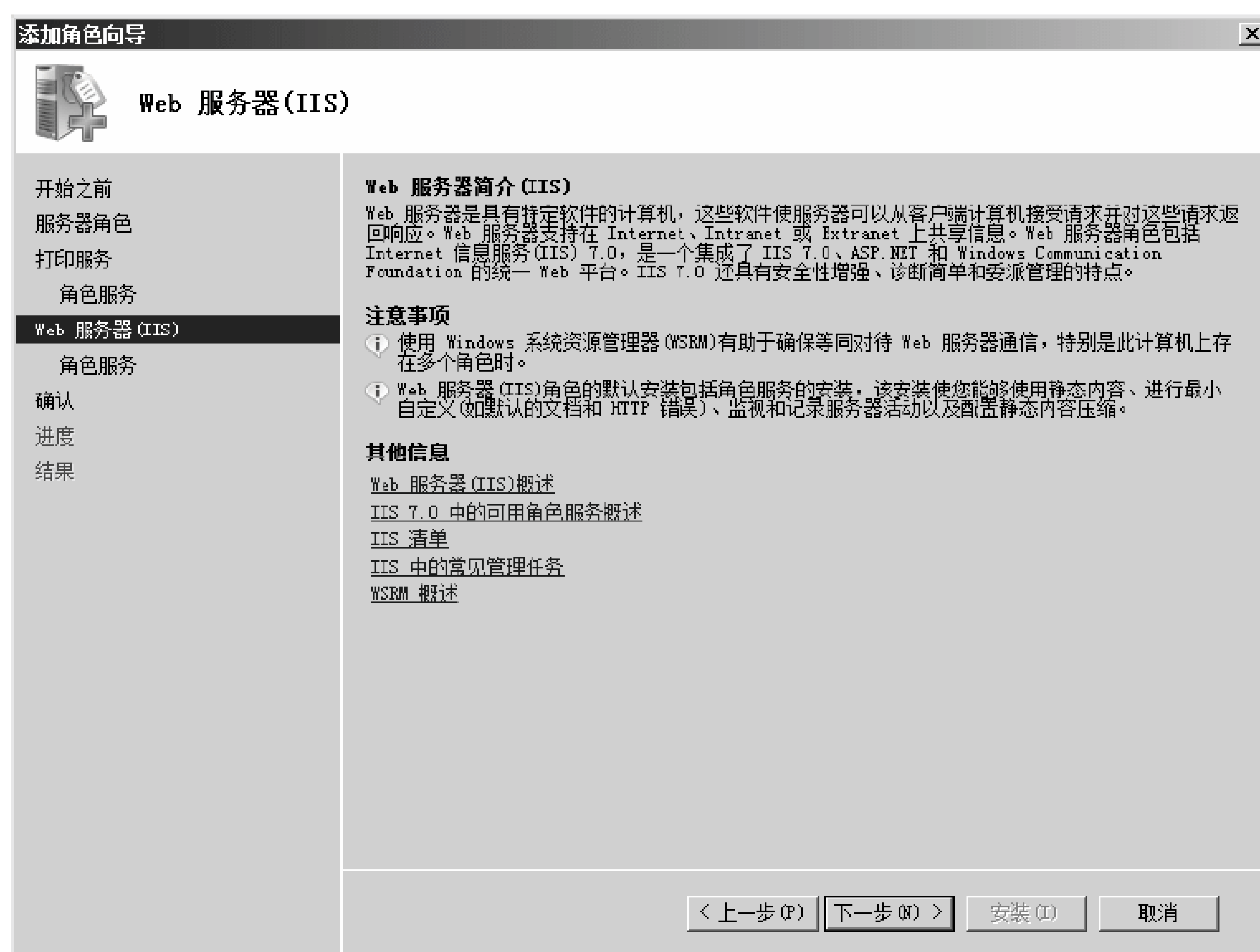


图 6-110　【Web 服务器（IIS）】对话框

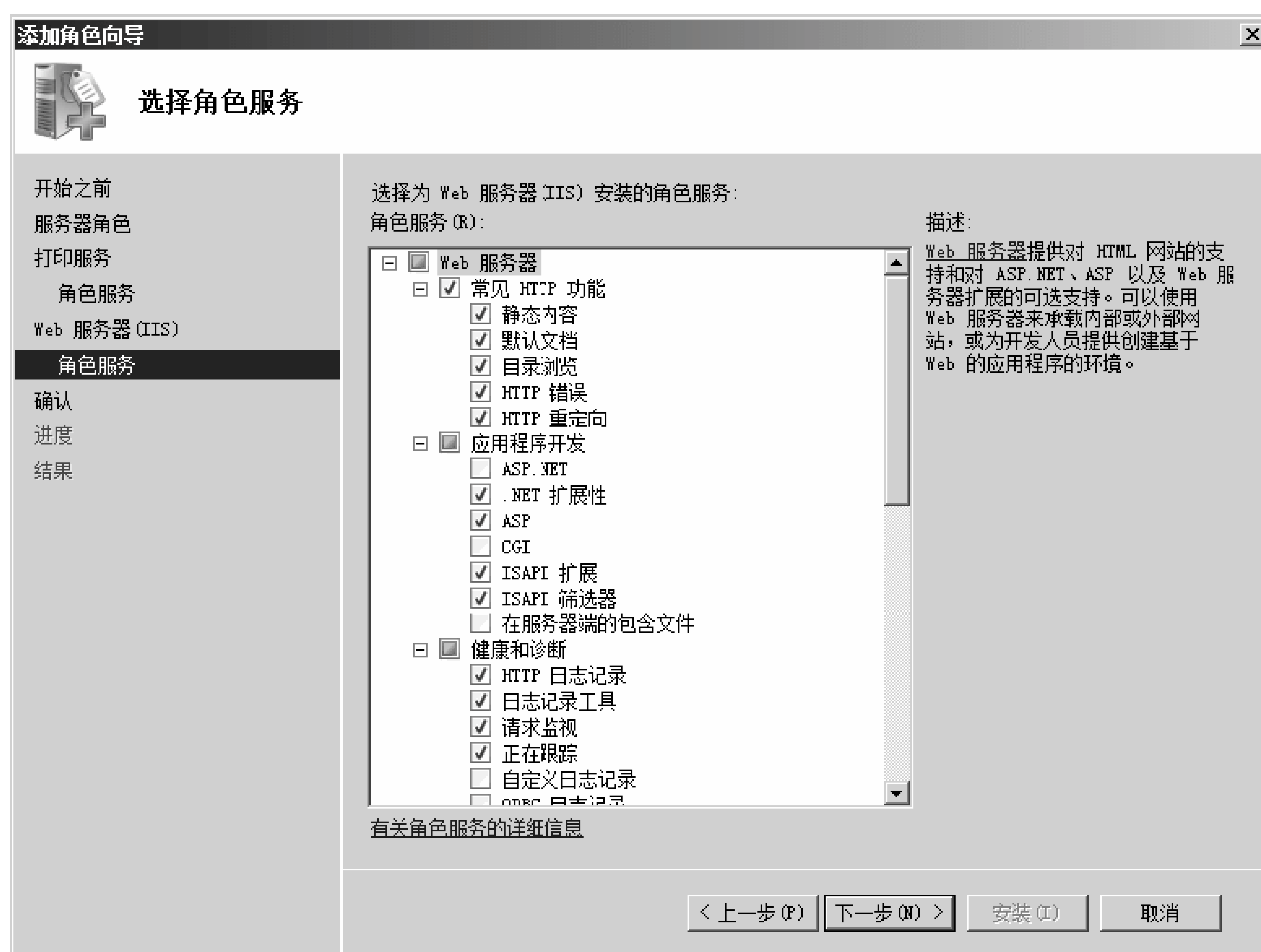


图 6-111 【选择角色服务】对话框

10 弹出【确认安装选择】对话框，显示安装打印服务器的配置信息，单击【安装】按钮，如图 6-112 所示。

11 弹出【安装进度】对话框，显示打印服务安装进度，如图 6-113 所示。



图 6-112 【确认安装选择】对话框



图 6-113 【安装进度】对话框

12 安装完成后弹出【安装结果】对话框，显示安装报告，单击【关闭】按钮，完成打印服务器的安装向导，如图 6-114 所示。



图 6-114 【安装结果】对话框

2. 添加打印机

打印机服务器安装好之后，需要手工添加打印机，添加的方法和所连打印机的类型有很大的关系，下面详细介绍添加直连打印机和网络打印机的操作步骤。

1）添加直连打印机

直连打印机的连接拓扑图如图 6-115 所示。

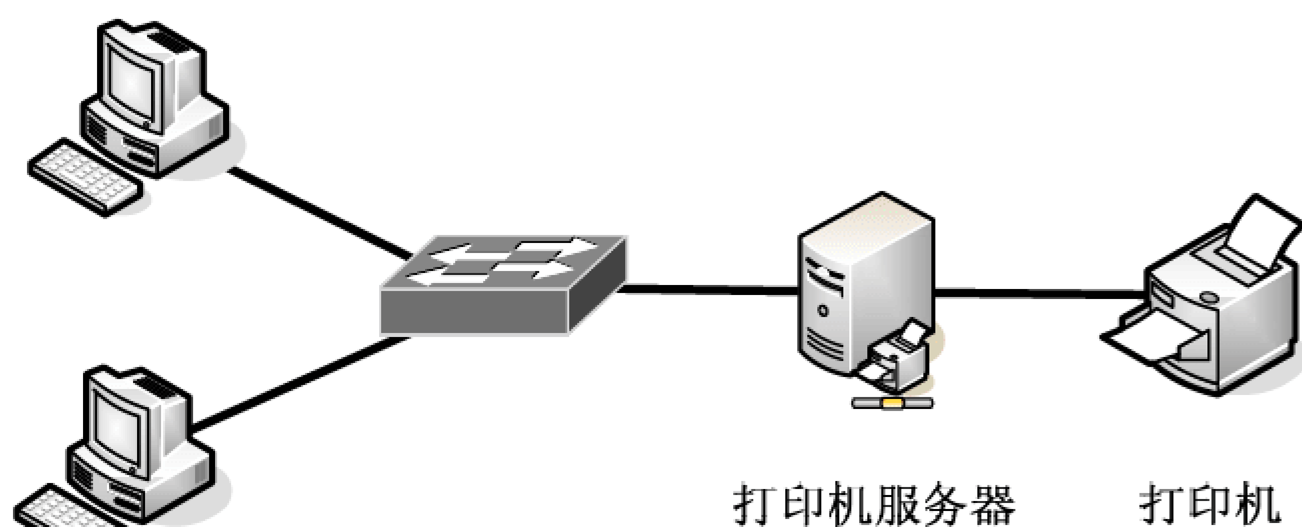


图 6-115　直连打印机拓扑图

01 选择【开始】➢【程序】➢【管理工具】➢【打印管理】命令，如图 6-116 所示。

02 弹出【打印管理】窗口，右击左侧选项列表中的【打印管理】➢【打印服务器】➢【WIN-K3VD3TJ2RME（本地）】➢【打印机】选项，在弹出的快捷菜单中选择【添加打印机】命令，如图 6-117 所示。



图 6-116　【开始】菜单选项



图 6-117　【打印管理】窗口

03 弹出【打印机安装】对话框，选中【使用现有的端口添加新打印机】单选按钮，在后侧选项列表中选择使用的打印机端口，一般打印机连接好后都会自动匹配，单击【下一步】按钮，如图 6-118 所示。

04 弹出【打印机驱动程序】对话框，选择安装打印机驱动程序的方法，选中【安装新驱动程序】单选按钮，单击【下一步】按钮，如图 6-119 所示。

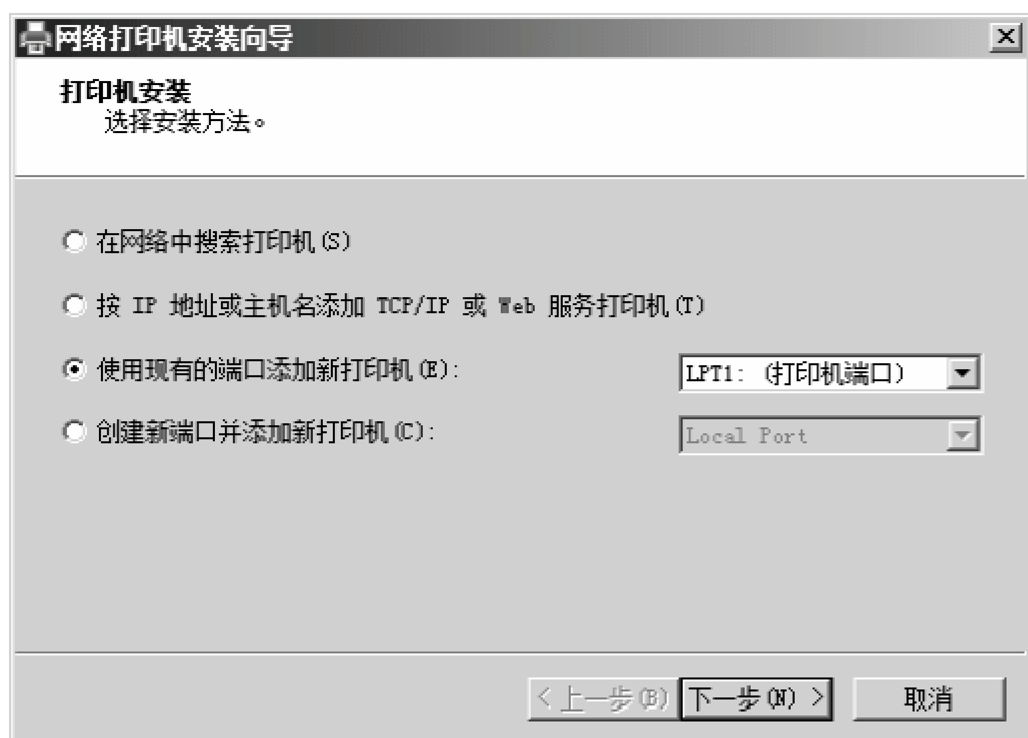


图 6-118　选择安装方法

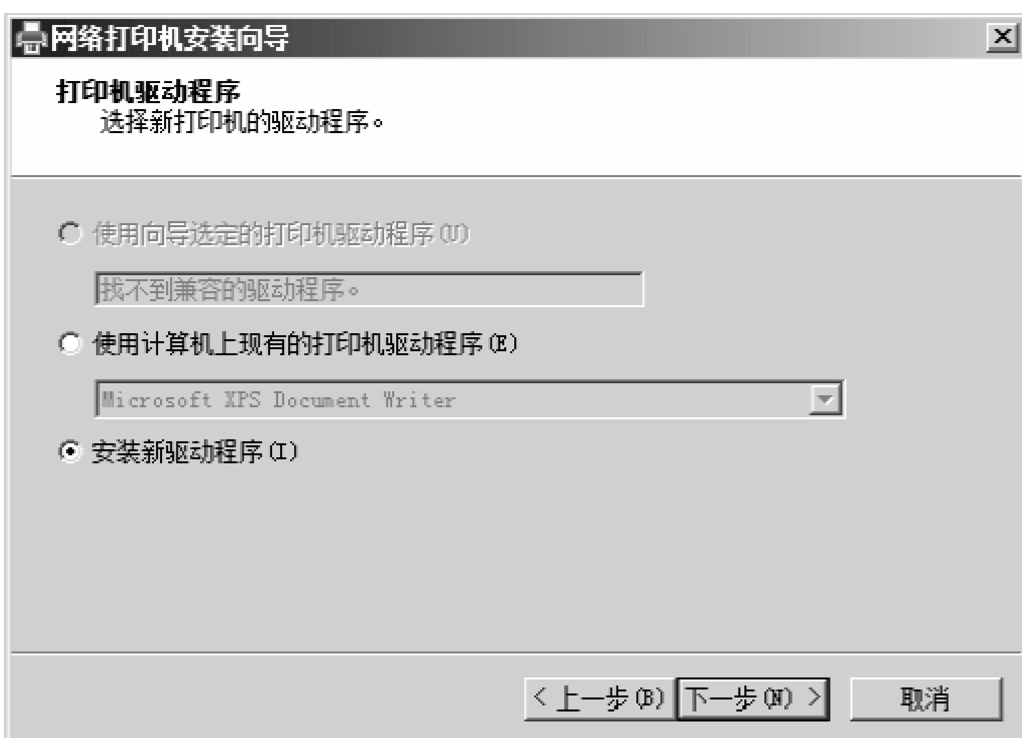


图 6-119　【打印机驱动程序】对话框

05 弹出【打印机安装】对话框，在【厂商】列表框中选择企业使用的打印机厂商，在【打印机】列表框中选择使用的打印机型号，如果本地没有匹配型号可以将该打印机的驱动光盘放入光驱，并单击【从磁盘安装】按钮安装驱动，选择完成后单击【下一步】按钮，如图 6-120 所示。

06 弹出【打印机名称和共享设置】对话框，【打印机名】默认为设备型号，可手动修改。由于是企业打印机，需要选中【共享此打印机】复选框，【共享名称】默认为设备名，建议使用具有特殊意义的名称，如使用地理位置命名，设置完成后单击【下一步】按钮，如图 6-121 所示。

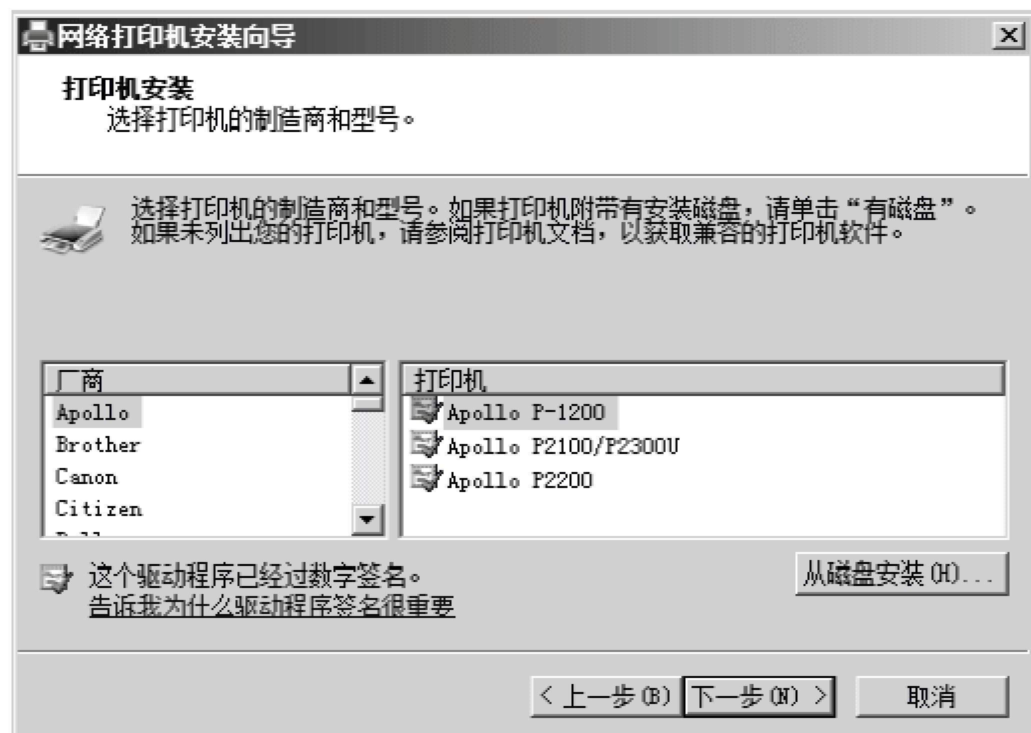


图 6-120　选择打印机的制造商和型号

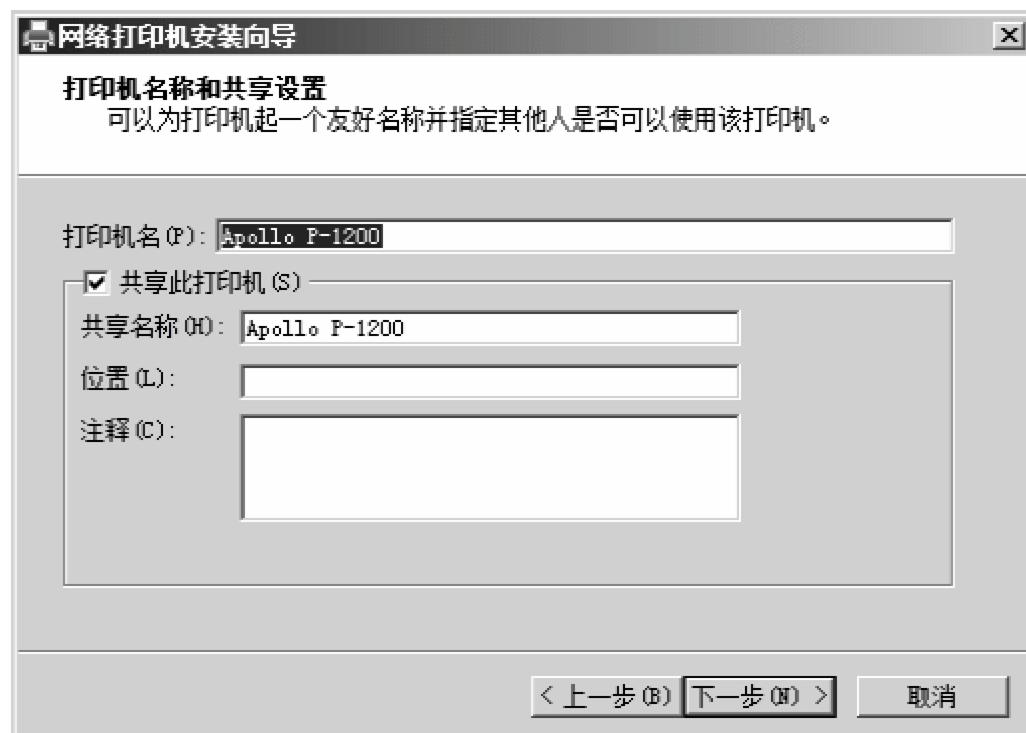


图 6-121　【打印机名称和共享设置】对话框

07 弹出【找到打印机】对话框，显示连接的打印机信息，单击【下一步】按钮，如图 6-122 所示。

08 打印机添加成功，弹出【正在完成网络打印机安装向导】对话框，为了验证打印机是否安装正确，可选中【打印测试页】复选框，本实例不做操作，单击【完成】按钮，结束向导，如图 6-123 所示。

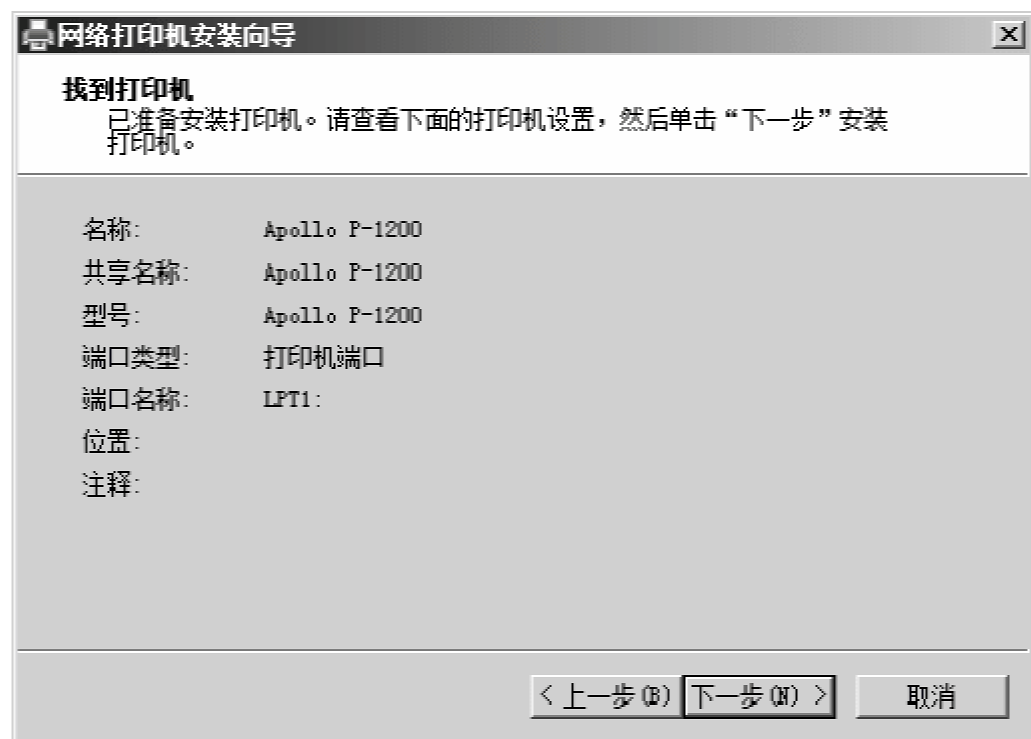


图 6-122　【找到打印机】对话框

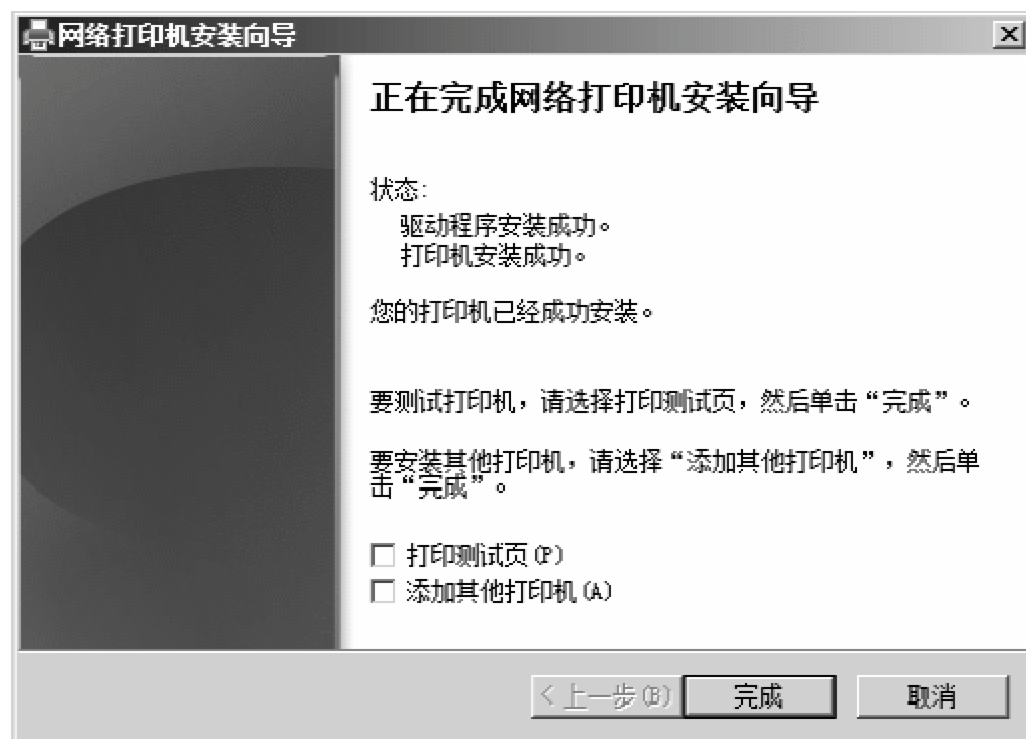


图 6-123　【正在完成网络打印机安装向导】对话框

2）添加网络打印机

网络打印机的连接拓扑图如图 6-124 所示。

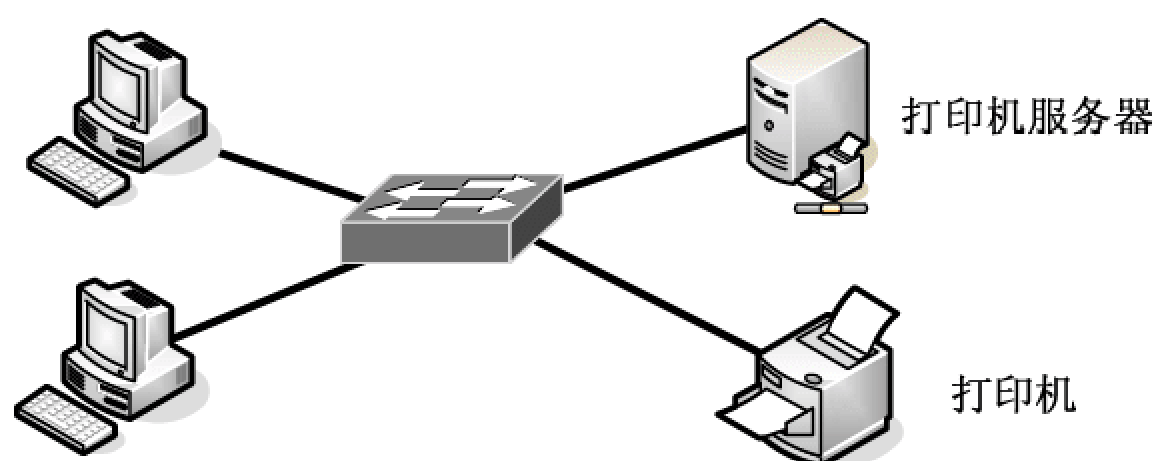


图 6-124　网络打印机网络拓扑图

01 弹出【打印管理】窗口，右击左侧选项列表中的【打印管理】➢【打印服务器】➢【WIN-K3VD3TJ2RME（本地）】➢【打印机】选项，在弹出的快捷菜单中选择【添加打印机】命令，如图 6-117 所示。

02 弹出如图 6-118 所示的【打印机安装】对话框，选中【按 IP 地址或主机名添加 TCP/IP 或 Web 服务打印机】单选按钮，单击【下一步】按钮。

03 弹出【打印机地址】对话框，在【设备类型】下拉列表框中选择【TCP/IP 设备】选项，在【打印机名称或 IP 地址】文本框中输入网络打印机的 IP 地址，【端口名】为本地打印机接口标识，默认和网络打印机 IP 地址一样，单击【下一步】按钮，如图 6-125 所示。

04 弹出【检测 TCP/IP 端口】对话框，自动检测网络打印机，如图 6-126 所示。

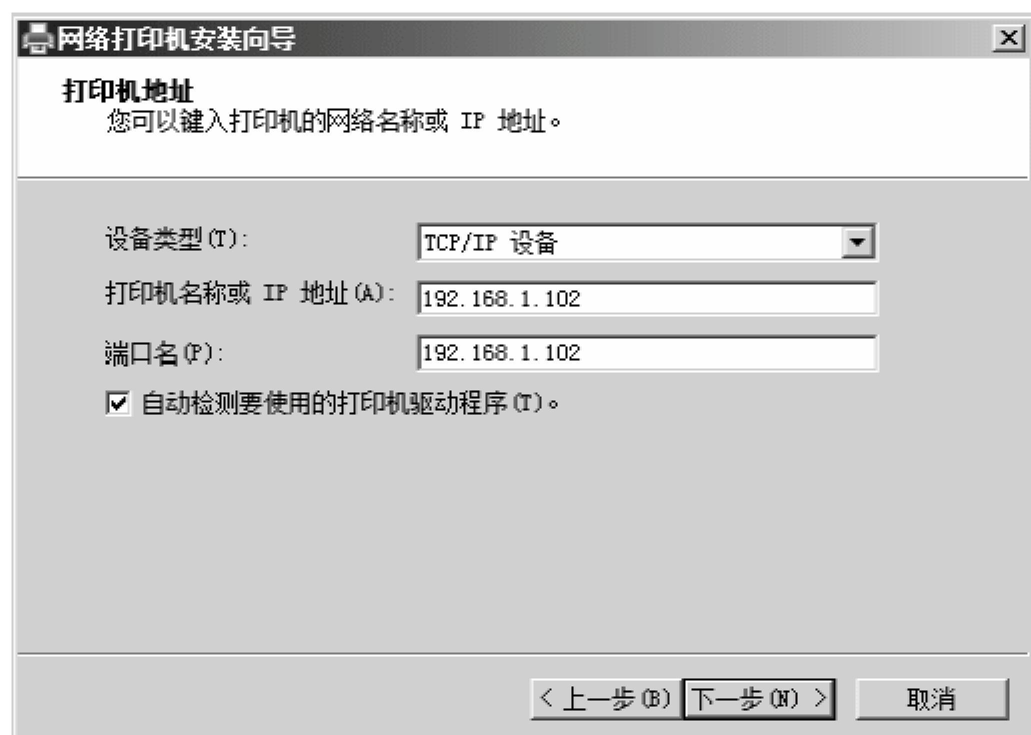


图 6-125　【打印机地址】对话框



图 6-126　【检测 TCP/IP 端口】对话框

05 检测失败会弹出【需要额外端口信息】对话框，可通过设置【设备类型】继续操作，如图 6-127 所示。

06 检测成功，弹出【打印机驱动程序】对话框，选择驱动安装方法，选中【安装新驱动程序】单选按钮，单击【下一步】按钮，如图 6-128 所示。

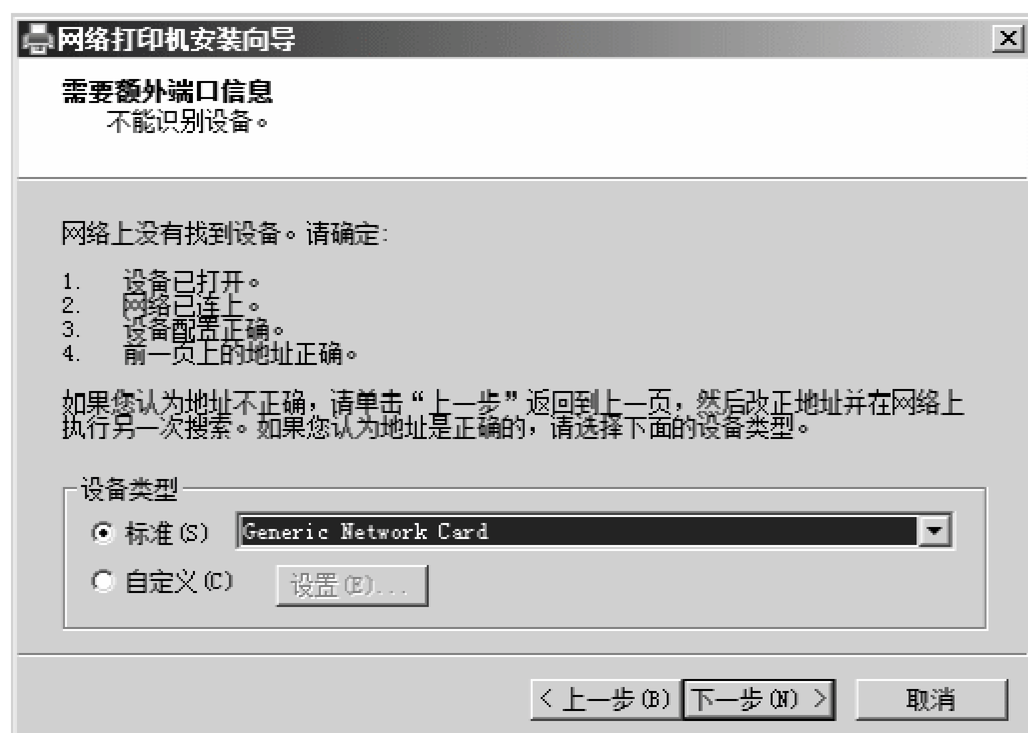


图 6-127　【需要额外端口信息】对话框

07 弹出【打印机安装】对话框，在【厂商】列表框中选择企业使用的打印机厂商，在【打印机】列表框中选择使用的打印机型号，如果本地没有匹配型号可以将该打印机的驱动光盘放入光驱，并单击【从磁盘安装】按钮安装驱动，选择完成后单击【下一步】按钮，如图 6-120 所示。

08 弹出【打印机名称和共享设置】对话框，【打印机名】默认为设备型号，可手动修改。由于是企业打印机，需要选中【共享此打印机】复选框，【共享名称】默认为设备名，建议使用具有特殊意义的名称，如使用地理位置命名，设置完成后单击【下一步】按钮，如图 6-121 所示。

09 弹出【找到打印机】对话框，显示连接的打印机信息，单击【下一步】按钮，如图 6-128 所示。

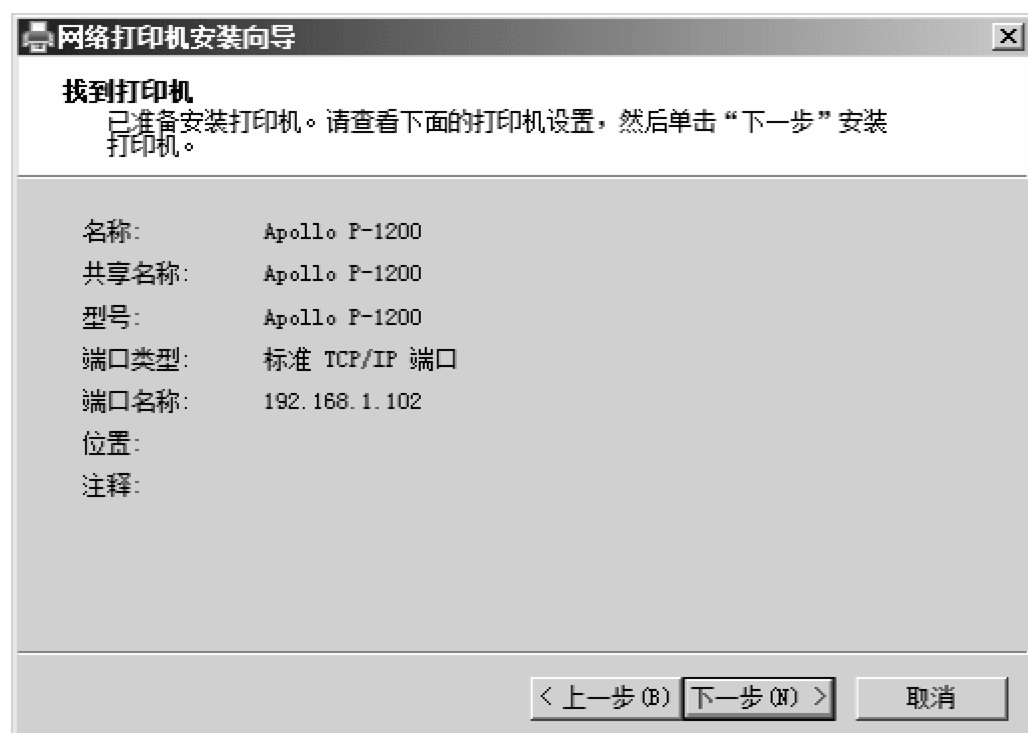


图 6-128　【找到打印机】对话框

10 打印机添加成功，弹出【正在完成网络打印机安装向导】对话框，为了验证打印机是否安装正确，可选中【打印测试页】复选框，本实例不做操作，单击【完成】按钮，结束向导，如图 6-123 所示。

3. 管理打印机

打印机添加完成后，需要进行简单的管理，可以通过打印机管理程序完成该工作，具体操作方法介绍如下。

01 打开【打印管理】窗口，在左侧选项列表中选择【打印机】选项，右击右侧已安装的打印机名称，在弹出的快捷菜单中选择【打开打印机队列】命令，如图 6-129 所示。

02 弹出【Apollo P-1200】窗口，显示目前有一个正在打印的文件，右击该文件，在弹出的快捷菜单中选择【属性】命令，如图 6-130 所示。



图 6-129 【打印管理】窗口



图 6-130 【Apollo P-1200】窗口

03 弹出【文档 属性】对话框，显示了该打印文件的常规打印属性，以及打印布局和打印纸张设置，如图 6-131 所示。

04 右击选择的打印机，在弹出的快捷菜单中选择【属性】命令，如图 6-132 所示。



图 6-131 【文档 属性】对话框



图 6-132 【打印管理】窗口

05 弹出【Apollo P-1200 属性】对话框，选择【常规】选项卡，显示了当前打印机的名称和打印功能，单击【打印首选项】按钮，如图 6-133 所示。

06 弹出【Apollo P-1200 打印首选项】对话框，选择【布局】选项卡，其中显示了打印纸张的布局方向，默认是纵向；还有打印文档内容的顺序，默认为从前向后打印；页面格式中【每张纸打印的页数】下拉列表框，如果设置为 2，表示原来两页的内容会在一张纸中缩小打印出来，是一种实现缩印的方法，如图 6-134 所示。



图 6-133　【Apollo P-1200 属性】对话框

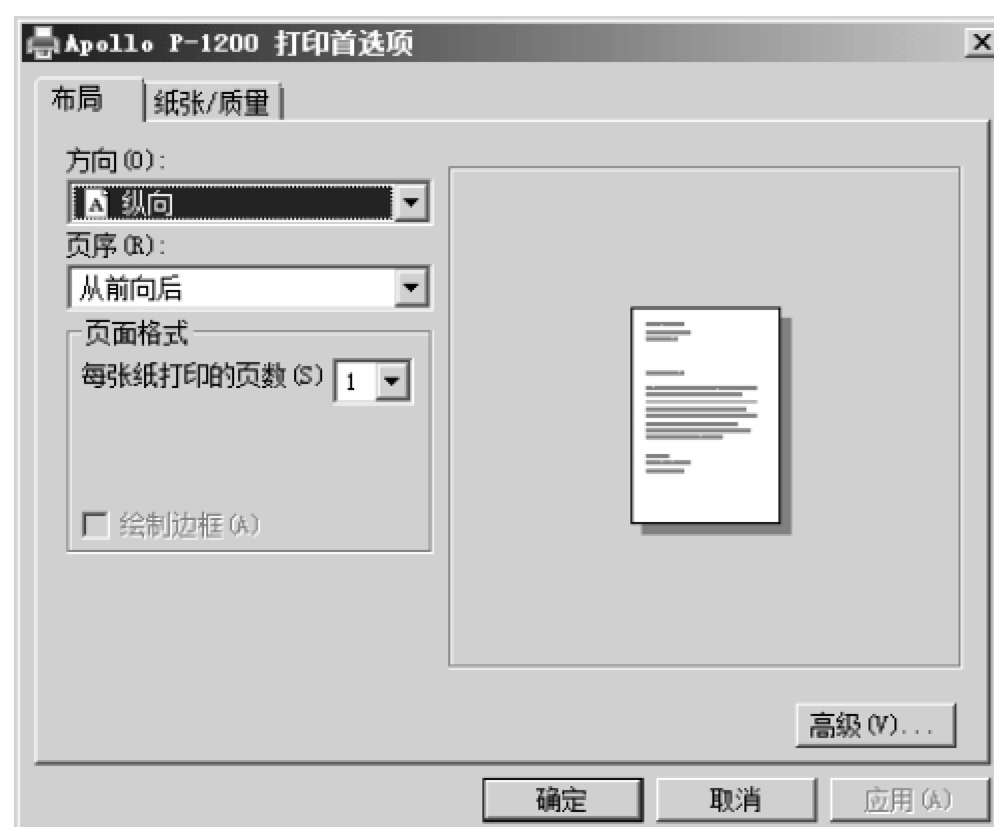


图 6-134　【Apollo P-1200 打印首选项】对话框

07 选择【Apollo P-1200 打印首选项】对话框中的【纸张/质量】选项卡，可以对纸张和其质量进行设置，一般采用默认配置。单击【高级】按钮可以对纸张和质量做更多的配置，如图 6-135 所示。

08 弹出【Apollo P-1200 高级选项】对话框，可对【纸张/输出】、【图形】和【文档选项】等内容进行配置，配置完成后单击【确定】按钮，如图 6-136 所示。



图 6-135　【纸张/质量】选项卡

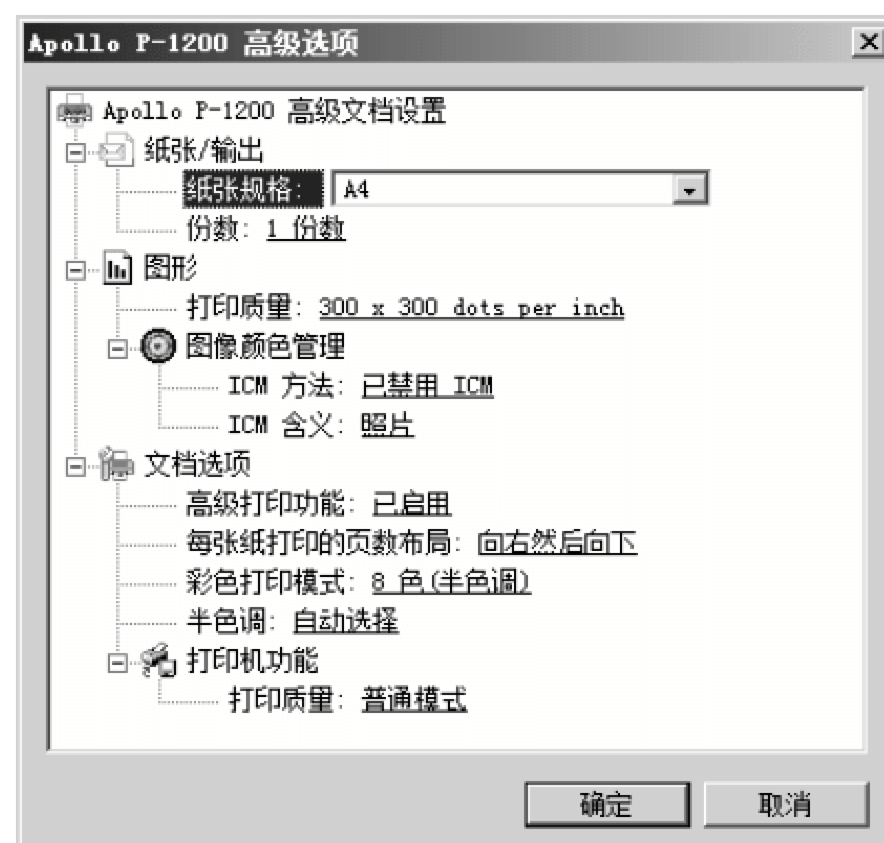


图 6-136　【Apollo P-1200 高级选项】对话框

09 在【Apollo P-1200 属性】对话框中选择【共享】选项卡，可以对本打印机设置共享，共享名如图 6-137 所示。

10 选择【端口】选项卡，当打印机硬件设备更换连接本地打印机服务器的接口时，可以通过该选项卡进行修改，列表中已经存在的可以直接选择，如果没有的可以通过单击【添加端口】按钮进行添加。如果想让多台打印机动态分担打印任务，可以同时选中这几台打印机的【启用打印机池】复选框，一般像打印社或出版社会启用该功能，如图 6-138 所示。



图 6-137 【共享】选项卡



图 6-138 【端口】选项卡

11 选择【高级】选项卡，首先可以设定打印机允许使用的时间范围，默认为【始终可以使用】，同时可以为打印机设置优先级，一般优先级越高，发送的打印任务越有优先打印的权利，其他内容一般采用默认，如图 6-139 所示。

12 选择【安全】选项卡，可以设置允许使用该打印机的本地账户，以及其所拥有的使用权限，默认 Everyone 组的账户只拥有打印权限，管理员组的账户拥有所有权限，如图 6-140 所示。

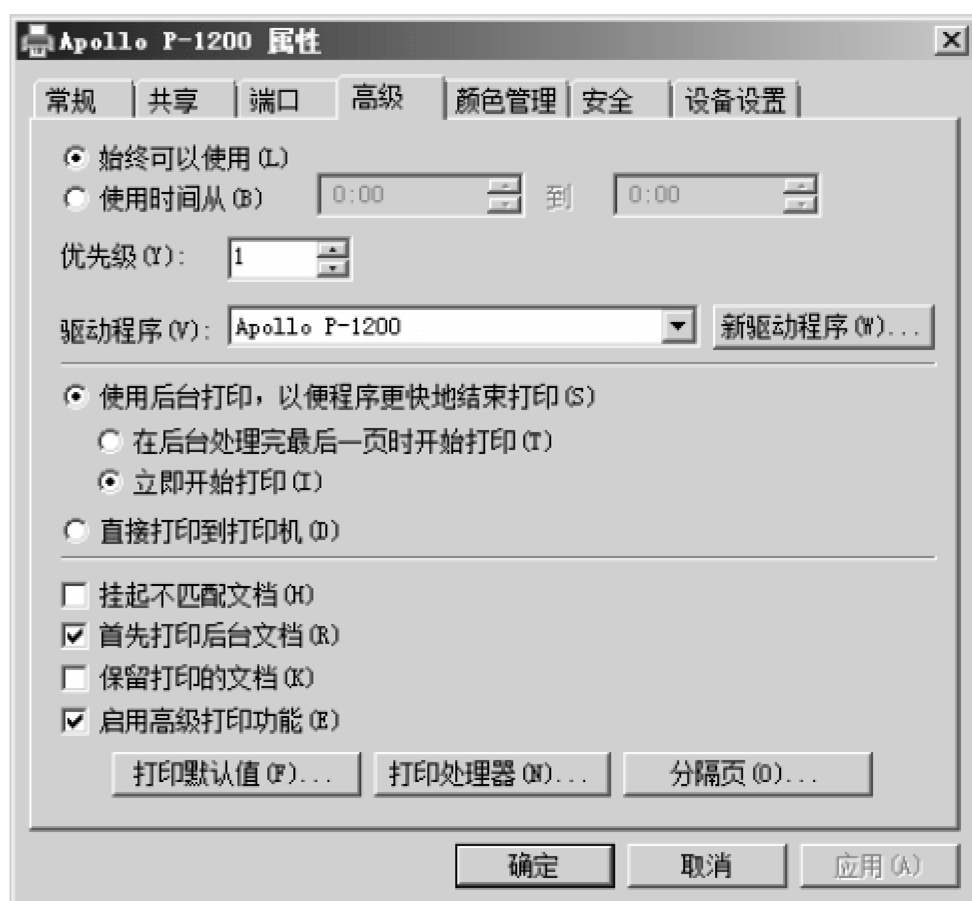


图 6-139 【高级】选项卡

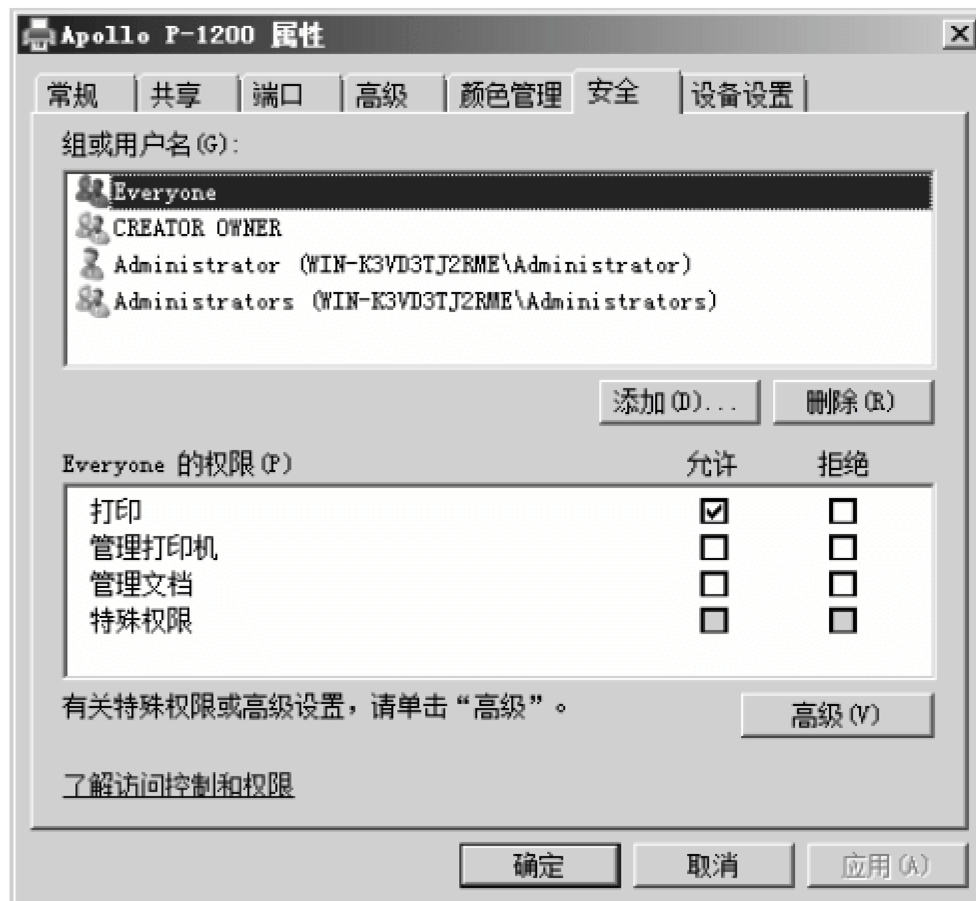


图 6-140 【安全】选项卡

6.5.3 项目实战 8：实现打印机全网共享使用

在局域网中为了方便所有员工能够通过自己的办公计算机直接使用企业打印机，可以将企业打印机做共享设置，这样就可以实现更快捷地使用打印机。上节已经介绍了打印机服务的共享设置，下面详细介绍客户机如何使用企业共享打印机，具体操作步骤如下。

01 在客户机上选择【开始】➢【设置】➢【打印机】命令，如图 6-141 所示。

02 打开【打印机】窗口，双击【添加打印机】选项，如图 6-142 所示。



图 6-141 开始菜单选项

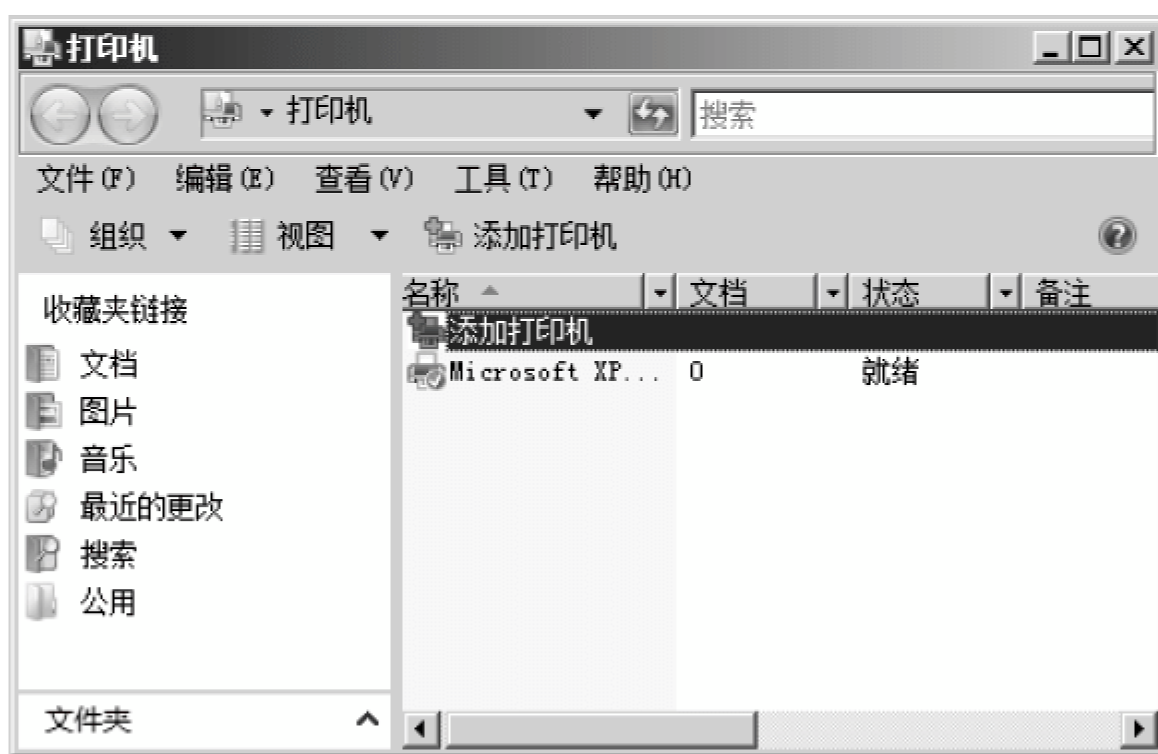


图 6-142 【打印机】窗口

03 弹出【选择本地或网络打印机】对话框，单击【添加网络、无线或 Bluetooth 打印机】链接，如图 6-143 所示。

04 弹出【正在搜索可用的打印机】对话框，开始搜索网络打印机，可能会搜索不到，直接单击【我需要的打印机不在列表中】链接，如图 6-144 所示。

05 弹出【按名称或 TCP/IP 地址查找打印机】对话框，在【按名称选择共享打印机】文本框中输入网络中已安装并共享的打印机，格式为“\\打印服务器 IP 或主机名\打印机共享名”，同时也可以单击【浏览】按钮，直接进行网络搜索，如图 6-145 所示。

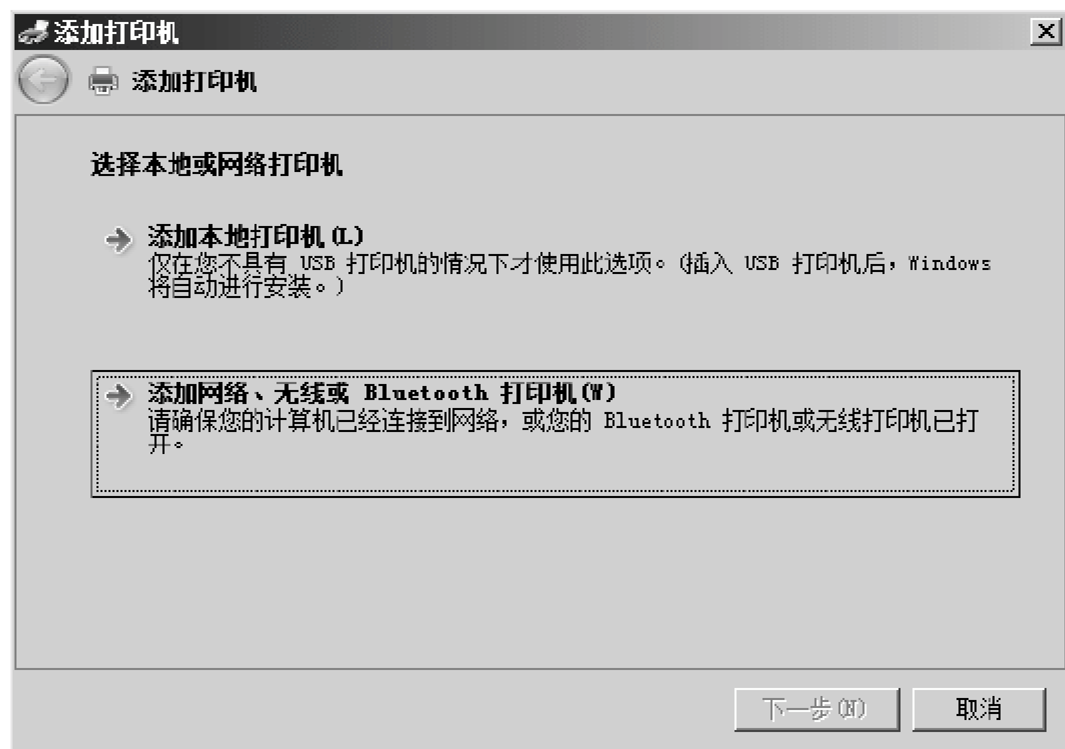


图 6-143 【选择本地或网络打印机】对话框

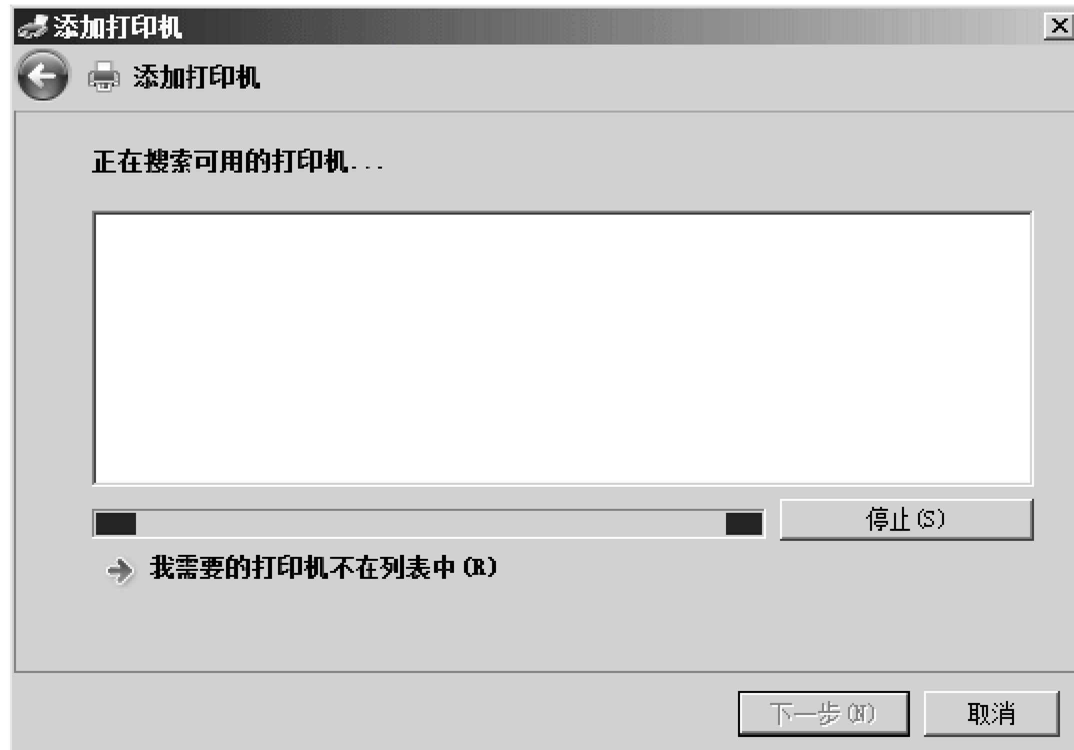


图 6-144 【正在搜索可用的打印机】对话框

06 单击【浏览】按钮后，弹出【请选择希望使用的网络打印机并单击“选择”以与之连接】对话框，扫描后网络中有两台主机，双击安装打印机的主机名，如图 6-146 所示。



图 6-145　指定查找打印机的方法

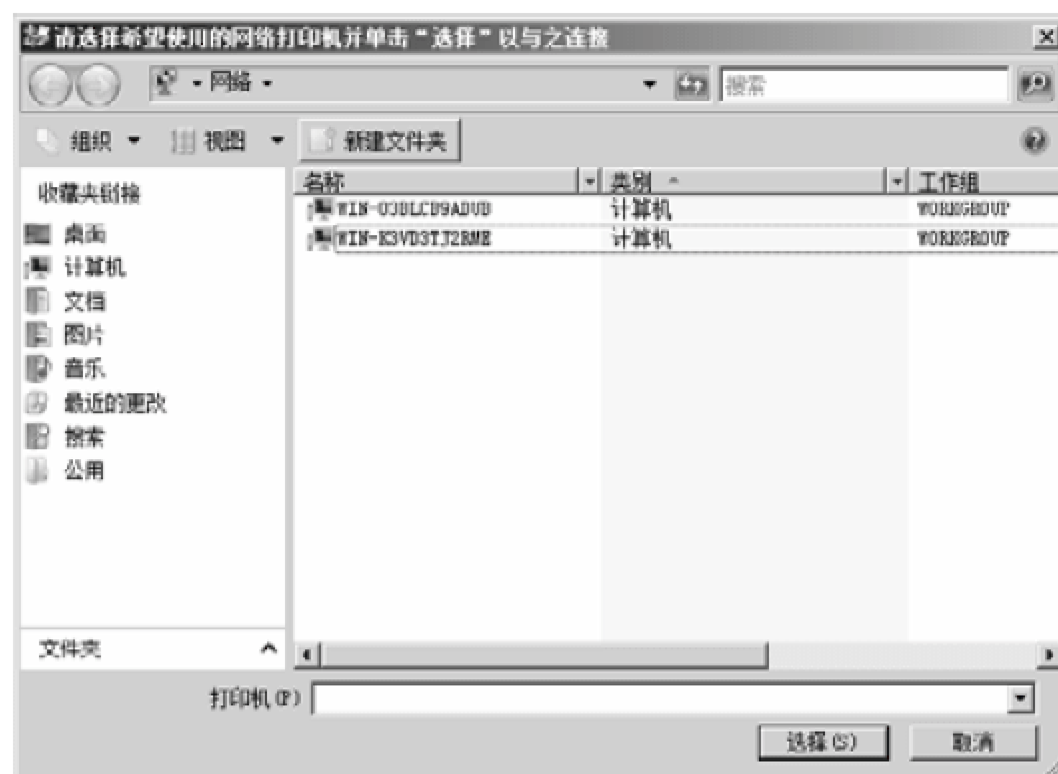


图 6-146　选择共享打印机的服务器

07 显示网络主机安装的打印机列表，选择后在【打印机】文本框显示打印机的共享名，单击【选择】按钮，如图 6-147 所示。

08 返回【按名称或 TCP/IP 地址查找打印机】对话框，共享打印机选择成功，单击【下一步】按钮，如图 6-148 所示。



图 6-147　选择共享的打印机



图 6-148　共享打印机指定成功

09 弹出【Windows 打印机安装】提示框，自动连接目标打印机，如图 6-149 所示。

10 连接成功，弹出【键入打印机名称】对话框，选中【设置为默认打印机】复选框，单击【下一步】按钮，如图 6-150 所示。

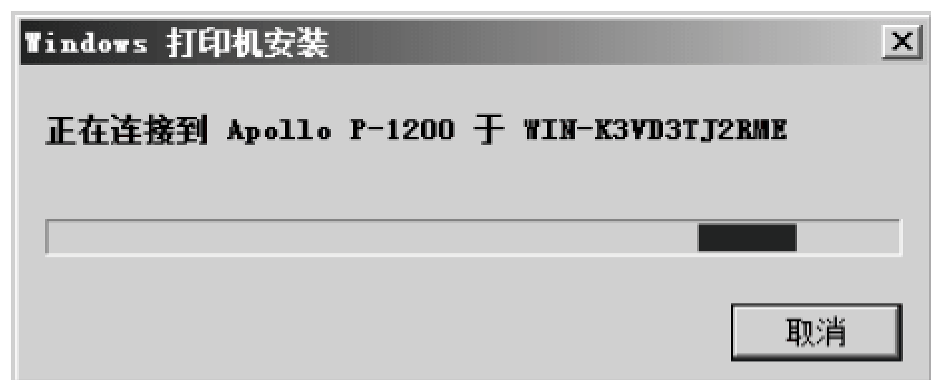


图 6-149　安装共享的打印机



图 6-150　【键入打印机名称】对话框

11 网络打印机添加成功，可以单击【打印测试页】按钮测试打印机，单击【完成】按钮，结束添加打印机向导，如图 6-151 所示。

12 返回【打印机】窗口，可以看到已连接的共享打印机，如图 6-152 所示。

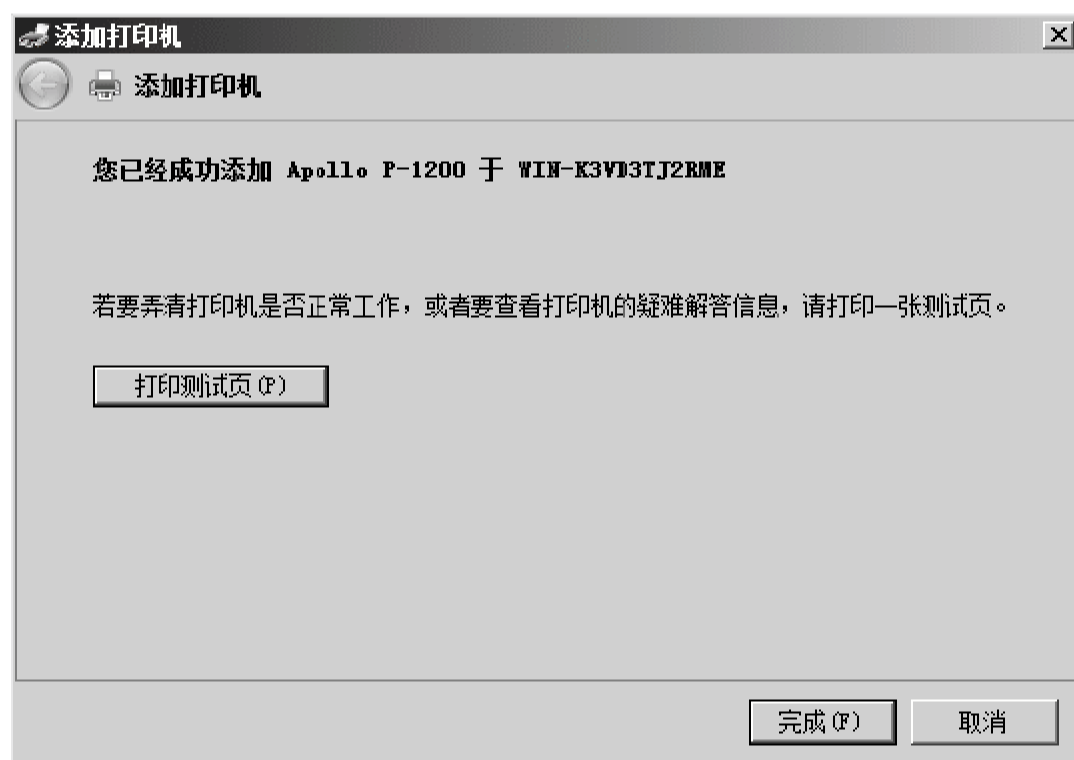


图 6-151　共享打印机连接成功

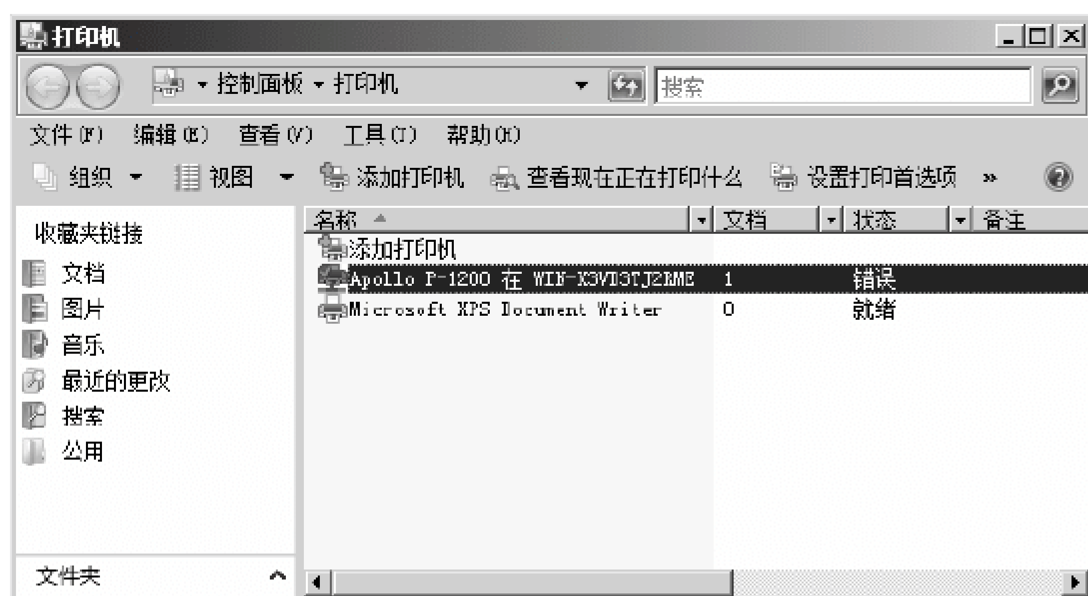


图 6-152　返回【打印机】窗口

6.6　专家答疑

（1）在使用 DHCP 服务器时，如果为多个 VLAN 配置了动态地址分配区间，这些 VLAN 的主机能自动获得地址吗？应当如何操作？

答：配置 DHCP 时，DHCP 服务器肯定在网络中的某一个虚拟局域网（VLAN）中，而 DHCP 动态地址分配过程中地址申请与分配信息都是通过广播发送的，广播流量不能跨越虚拟局域网通信，这么看来处于某一特定虚拟局域网的 DHCP 服务器不可能通过广播信息向其他 VLAN 的主机分配 IP 地址。

想要解决这个问题，就要从能够实现多个 VLAN 互通的三层交换机或者单笔路由器着手，在这些中间设备上需要实现 DHCP 中继代理，实现 DHCP 请求的代理转发。如果是三层交换机，需要在三层交换机的每一个 VLAN 中配置如下命令。

```
Switch (config)#interface VLAN [VLAN number]
Switch (config-if)#ip helper-address   [dhcp server ip]   //指定 DHCP 服务器地址
```

（2）在配置打印机服务的时候，总有些员工的打印任务比较急，需要优先打印。如何实现这一部分员工优先打印呢？

答：在配置打印机服务器时，可以为一个打印机安装两次，产生两个打印机图标，如图 6-153 所示的 Apollo P2200 打印机。



图 6-153　Apollo P2200 打印机安装了两次

对两个打印机分别做属性修改，打开属性对话框，在【高级】选项卡中分别配置【优先级】为“1”和“2”，如图 6-154 和图 6-155 所示。



图 6-154　配置优先级为 1

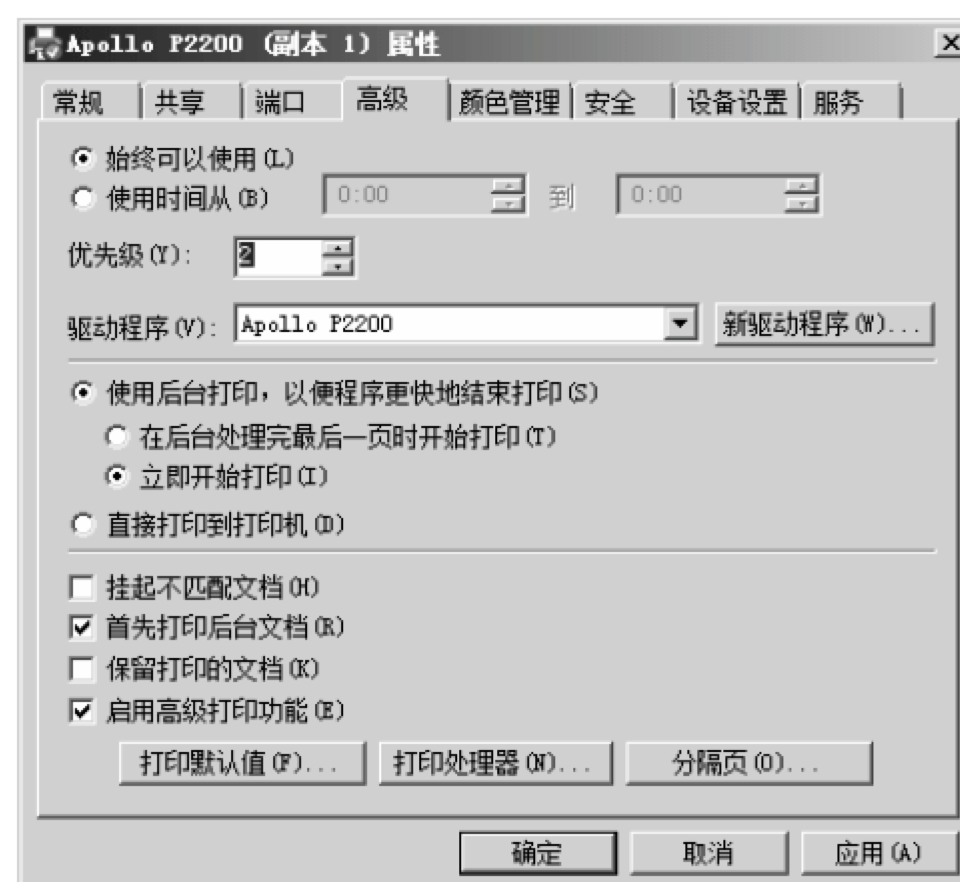


图 6-155　配置优先级为 2

将优先级设置为 1 的打印机连接图标分享给需要优先打印的员工，不需要优先打印的员工使用优先级配置为 2 的共享打印机。

第 7 章　FTP 服务器搭建与维护

随着无纸化办公的流行，文件的呈现越来越电子化，为了方便文件的上传和下载，就需要用到 FTP 服务器。本章主要介绍 FTP 服务器的基本概念和如何使用 Serv-U 搭建企业服务器。

7.1　FTP 服务器概述

FTP 服务器是在网络中提供存储空间的计算机，依照 FTP 协议提供服务。下面来介绍一些 FTP 服务器的基本概念。

7.1.1　什么是 FTP 服务器

所谓 FTP（File Transfer Protocol）就是文件传输协议的简称，它主要是为了方便在网络中进行文件的上传和下载，并且可以随时对用户上传下载文件进行监控。

FTP 服务器的首要目标就是要实现文件传输，并且能够根据需求对用户上传和下载文件的权限进行管理。使用 FTP 服务器时必须先登录，这时候就需要用到合法的账户和密码，大多数的 FTP 服务器都是针对不同的账户设置不同的操作权限来限制用户使用 FTP 的行为。

7.1.2　搭建 FTP 服务器的软件

常用的实现 FTP 服务的软件有很多，如 Serv-U、Vsftpd 等。其中 Vsftpd 是一个基于 GPL 发布的类似 UNIX 系统上使用的 FTP 服务器软件，Serv-U 是一个基于 Windows 系统使用最为广泛的 FTP 软件。本书中以 Serv-U 为案例讲解如何建立 FTP 服务器。

Serv-U 是一种被广泛应用的 FTP 服务器端软件，支持 Windows 系列系统，通过 Serv-U 可以设定多个 FTP 服务器，限定登录用户的权限、登录主目录及空间大小等，功能非常完备。

通过使用 Serv-U，用户能够将任何一台 PC 设置成一个 FTP 服务器，这样用户或者其他使用者就能够使用 FTP 协议，通过在同一网络的任何一台 PC 与 FTP 服务器连接，进行文件或目录的复制、移动、创建和删除等。

图 7-1 所示是 Serv-U 的管理控制台界面。



图 7-1　Serv-U 管理控制台界面

7.1.3　高校 FTP 服务器案例分析

某高校为了方便教师课程资料的管理和学生作业的提交，在学校内部建立了 FTP 服务器。其中对 FTP 服务器的具体要求有以下几个方面。

（1）教师访问 FTP 服务器使用的 IP 地址为 192.168.1.199，学生访问 FTP 服务器使用的地址为 172.16.1.254，两个 IP 地址网段不能通信。

（2）学生访问 FTP 服务器后，使用合法的账户和密码可以访问学生的作业目录，通过这个账户学生可以上传作业，但是不能删除作业目录中的任何内容。学生使用教师的账号登录后可以看到看到教师的课程资料，学生对教师的课程资料只能读取，不能写入或者删除。

（3）教师访问 FTP 服务器后，使用教师的账户登录，可以看到自己上传的文件，通过教师的账户教师可以对自己的目录写入和删除。另外为了方便教师更改作业，教师使用自己的账号登录后除了可以看到自己的文件和文件夹之外，还可以看到学生的作业目录，为了学生作业目录的安全起见，教师只能读取和写入不能删除。

（4）为了提高 FTP 服务器的运行效率，对学生和教师在 FTP 服务器上上传和下载数据的速率进行限制，同时对学生和教师使用 FTP 硬盘空间大小根据不同的情况进行限制。

经过以上的分析，不难发现，该学校需要建立一个 FTP 服务器，其中 FTP 服务器上要实现同一账户在多网段访问具有不同的权限，用户除了可以管理自己目录的内容外还可以管理自己目录之外的文件和文件夹。

7.2　项目实战：使用 Serv-U 搭建企业文件服务器

Serv-U 的软件版本从 Serv-U1.0 发展到现在的 Serv-U10，在继承了 Serv-U 的简单易操作的优秀传统基础上，Serv-U10 版本在功能和安全上都做了大量优化，使得 Serv-U 逐渐成为 Windows 系统上最为流行的 FTP 软件之一。

7.2.1　安装 Serv-U 软件

Serv-U 软件的安装过程比较简单，只需要根据提示进行安装即可。安装 Serv-U 软件的具体操作步骤如下。

01 双击 Serv-U 安装文件，弹出【选择安装语言】对话框，在语言下拉表框中选择【中文（简体）】选项，单击【确定】按钮，如图 7-2 所示。

02 弹出【安装向导—rv-U】对话框，单击【下一步】按钮继续安装 Serv-U 软件，如图 7-3 所示。

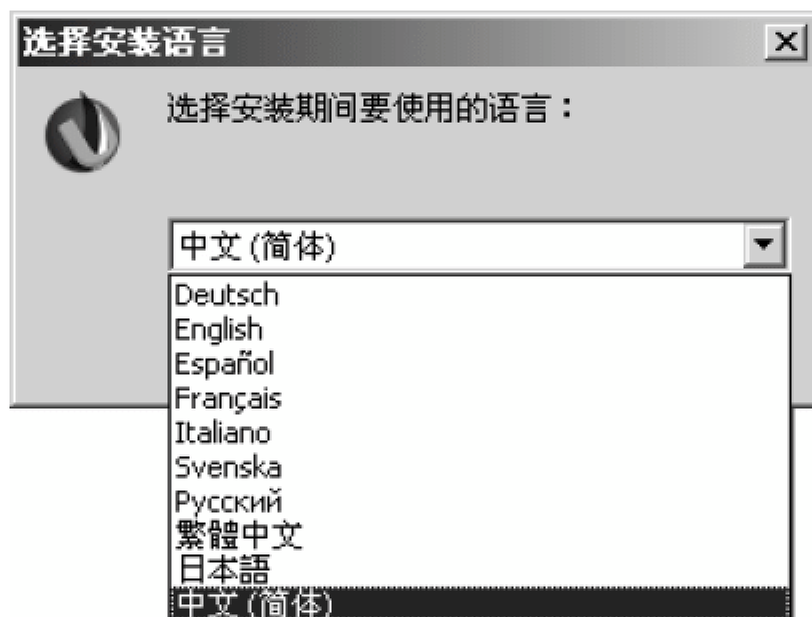


图 7-2　【选择安装语言】对话框



图 7-3　【安装向导 – Serv-U】对话框

03 弹出【许可协议】对话框，选中【我接受协议】单选按钮，表示同意 Serv-U 软件安装协议，单击【下一步】按钮，如图 7-4 所示。

04 弹出【选择目标位置】对话框，单击【浏览】按钮自定义安装路径，默认的安装路径为“C:\Program Files\RhinoSoft.com\Serv-U”，本实例采用默认安装路径，单击【下一步】按钮，如图 7-5 所示。

05 弹出【选择开始菜单文件夹】对话框，单击【浏览】按钮自定义 Serv-U 程序在开始菜单中创建的快捷方式的文件夹，本实例采用默认值 “Serv-U”文件夹，单击【下一步】按钮，如图 7-6 所示。

06 弹出【选择附加任务】对话框，分别选中【创建桌面图标】、【创建快速启动栏图标】和【将 Serv-U 作为系统服务安装】复选框，单击【下一步】按钮，如图 7-7 所示。

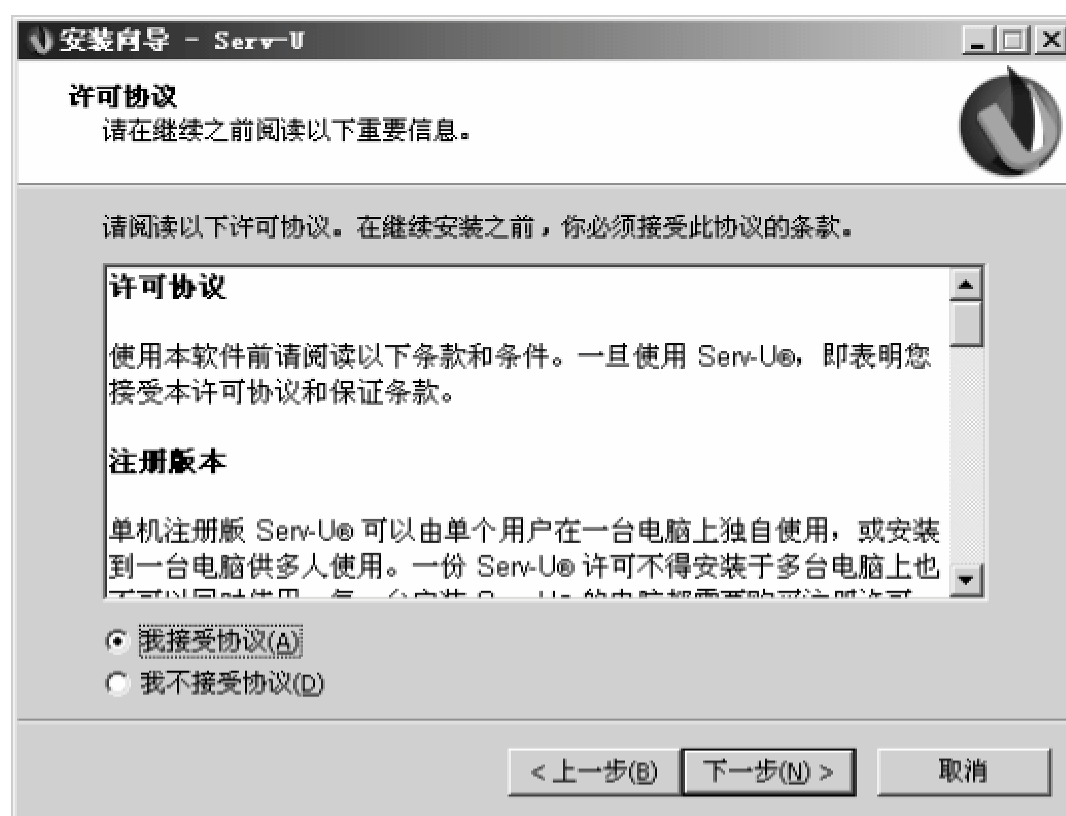


图 7-4 【许可协议】对话框



图 7-5 【选择目标位置】对话框

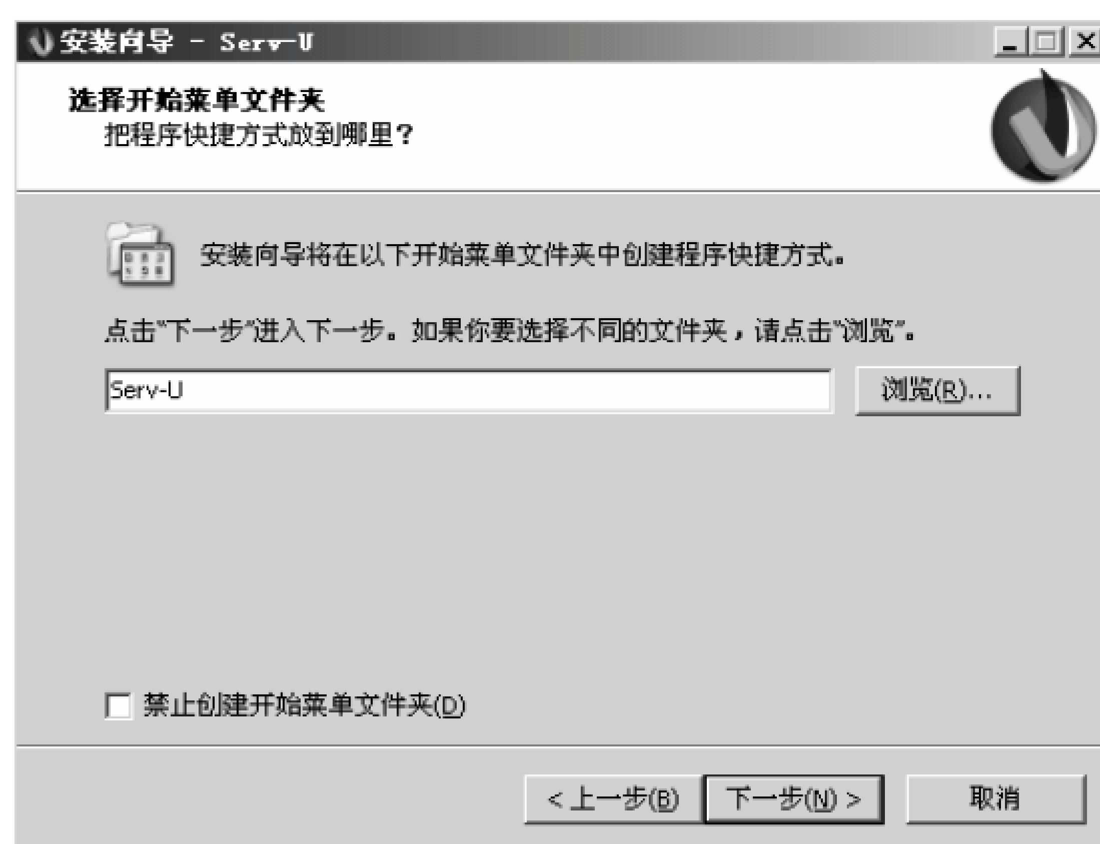


图 7-6 【选择开始菜单文件夹】对话框

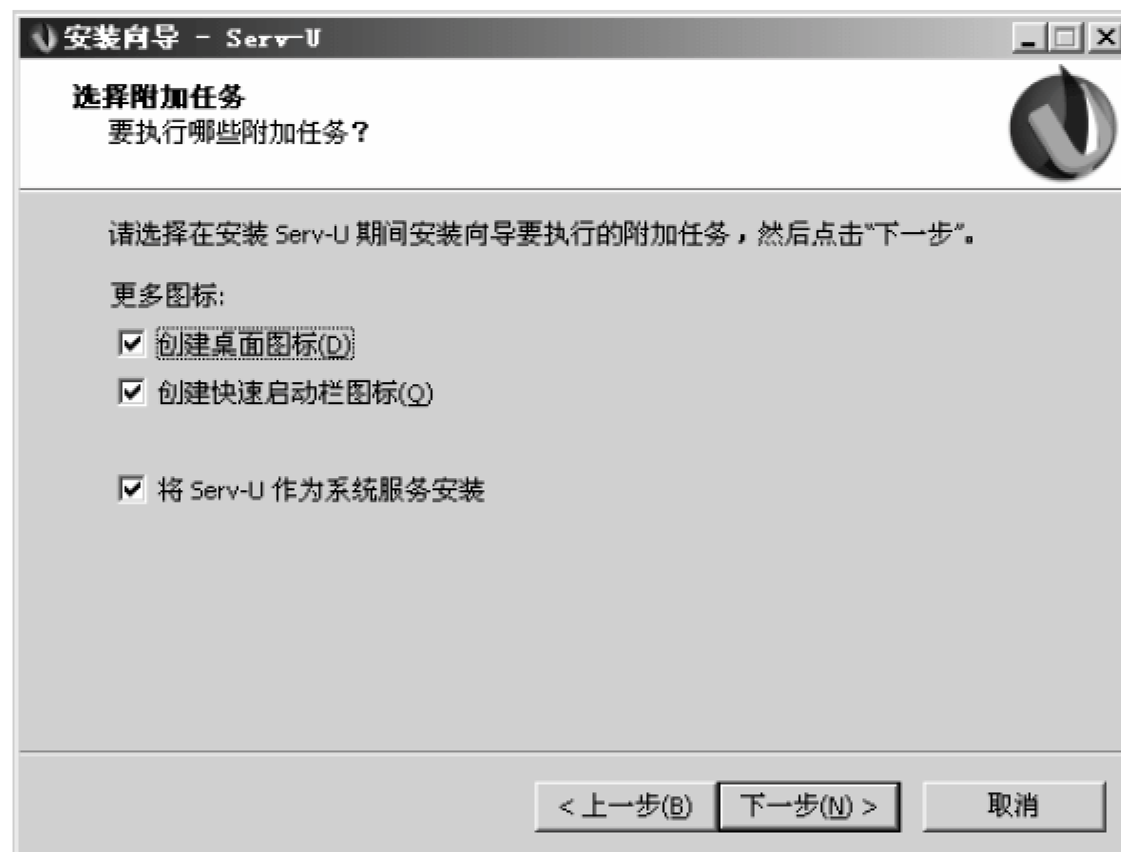


图 7-7 【选择附加任务】对话框

07 弹出【准备安装】对话框，显示安装信息，单击【安装】按钮，如图 7-8 所示。

08 弹出【正在安装】提示框，显示 Serv-U 安装进度，如图 7-9 所示。

09 安装过程结束，弹出【完成 Serv-U 安装】对话框，选中【启动 Serv-U 管理控制台】复选框，单击【完成】按钮完成 Serv-U 软件的安装，如图 7-10 所示。



图 7-8 【安装信息】对话框

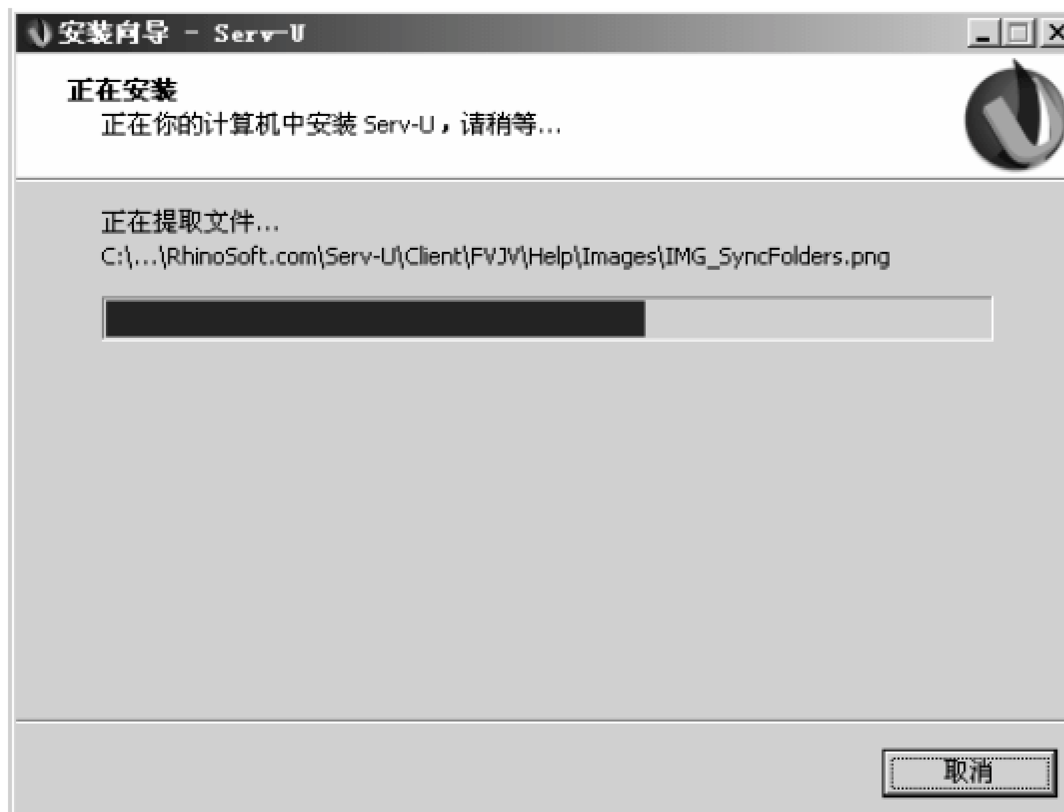


图 7-9 【安装进度】对话框



图 7-10　【完成 Serv-U 安装】对话框

7.2.2　为用户分配 FTP 账户及空间

Serv-U 安装完成后，就需要为每个用户分配账户和密码。Serv-U 可以针对不同的用户分配不同的主目录和权限，确保每个用户使用自己的账户登录后只能看到自己目录的内容，并且不同用户对自己目录的权限可以不同，下面首先规划 FTP 目录。

（1）人员分配：公司有两名员工苏红和王明，经理名字为王晓亮。账户分别为 sh、wm 和 wxl，密码统一为 123。

（2）权限分配：员工苏红对自己的目录具有读、写和删除的权利，员工王明对自己的目录具有读和写的权利，但是不能删除文件和文件夹，经理王晓亮对自己的目录有读、写和删除的权利，对自己部门员工的目录具有读和写的权利，但是不能删除。

（3）资源分配：为了合理使用 FTP 空间，限制员工可以使用 FTP 服务器 500M 硬盘空间，经理可以使用 FTP 服务器 1000M 硬盘空间。同时，员工使用 FTP 进行上传和下载文件的速率控制在 2Mb/s，经理使用 FTP 进行上传和下载文件的速率控制在 4Mb/s。

具体的 FTP 目录规划如图 7-11 所示。

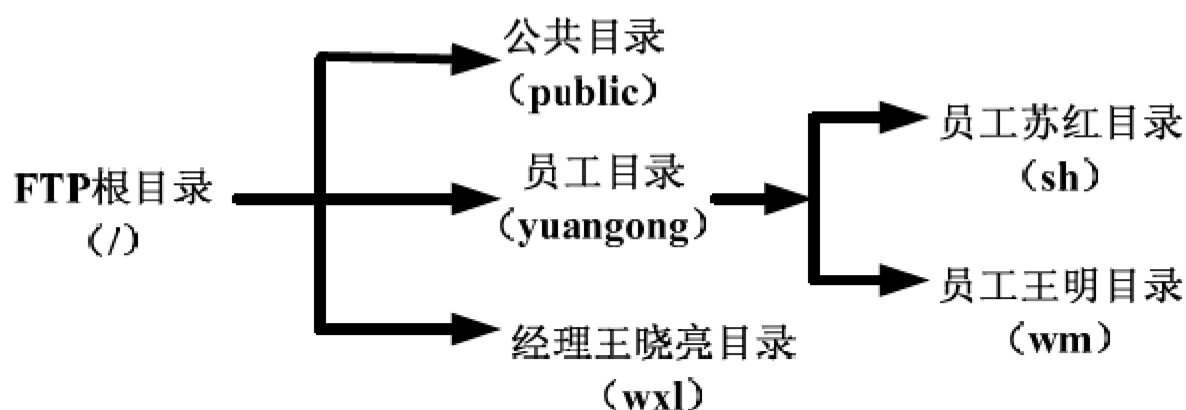


图 7-11　FTP 目录规划

使用 Serv-U 软件为多用户分配账户和空间的具体操作方法如下。

1. 为 Serv-U 创建匿名用户访问

为 Serv-U 创建匿名用户的具体操作步骤如下。

01 双击桌面上的 Serv-U 快捷方式图标，弹出【已启用 Windows Internet 增强的安全配置】提示框，因为 Windows Server 2003 系统的 IE 安全级别过高，单击【确定】按钮，如图 7-12 所示。

02 弹出【Serv-U】提示框，单击【是】按钮，建立 Serv-U 的第一个域，如图 7-13 所示。

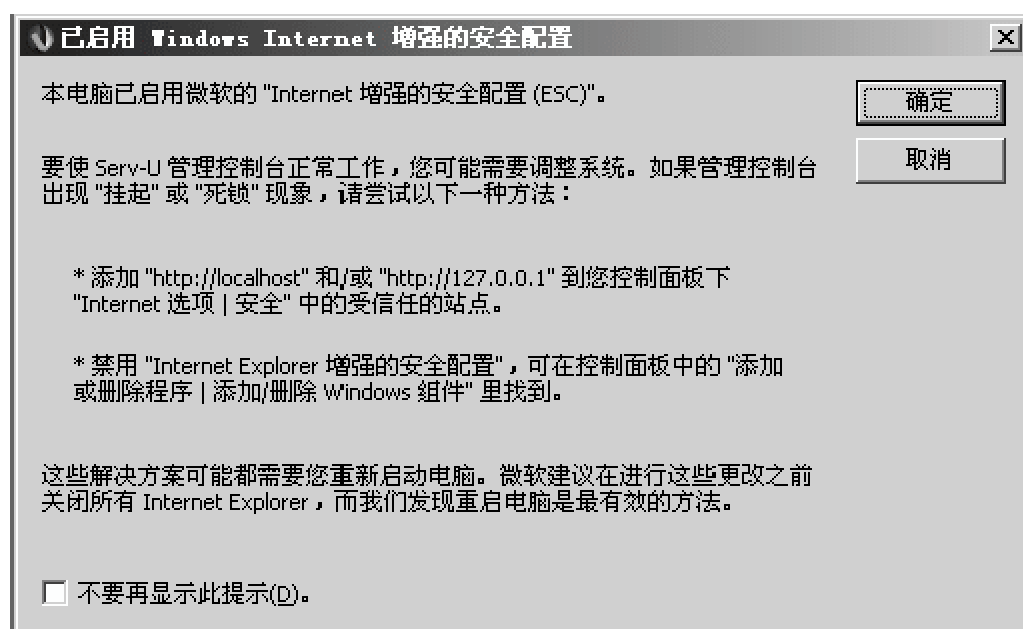


图 7-12 【已启用 Windows Internet 增强的安全配置】对话框

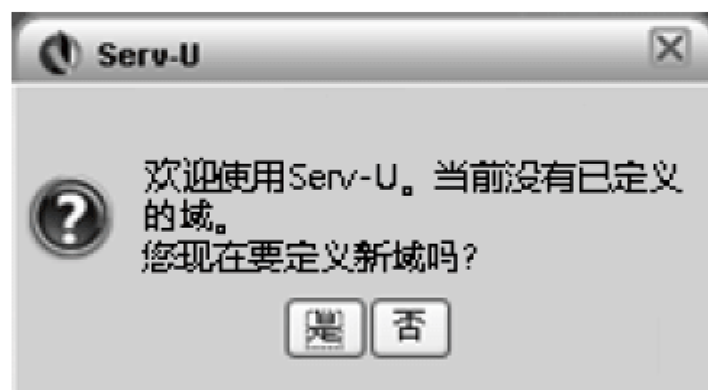


图 7-13 【Serv-U】提示框

03 弹出【域向导 – 步骤 1 总步骤 4】对话框，在【名称】文本框中输入域名称，本实例中输入域名称为“192.168.1.200”，选中【启用域】复选框，如图 7-14 所示，单击【下一步】按钮。

04 弹出【域向导 – 步骤 2 总步骤 4】对话框，选中【FTP 和 Explicit SSL/TLS】复选框，如图 7-15 所示，单击【下一步】按钮。

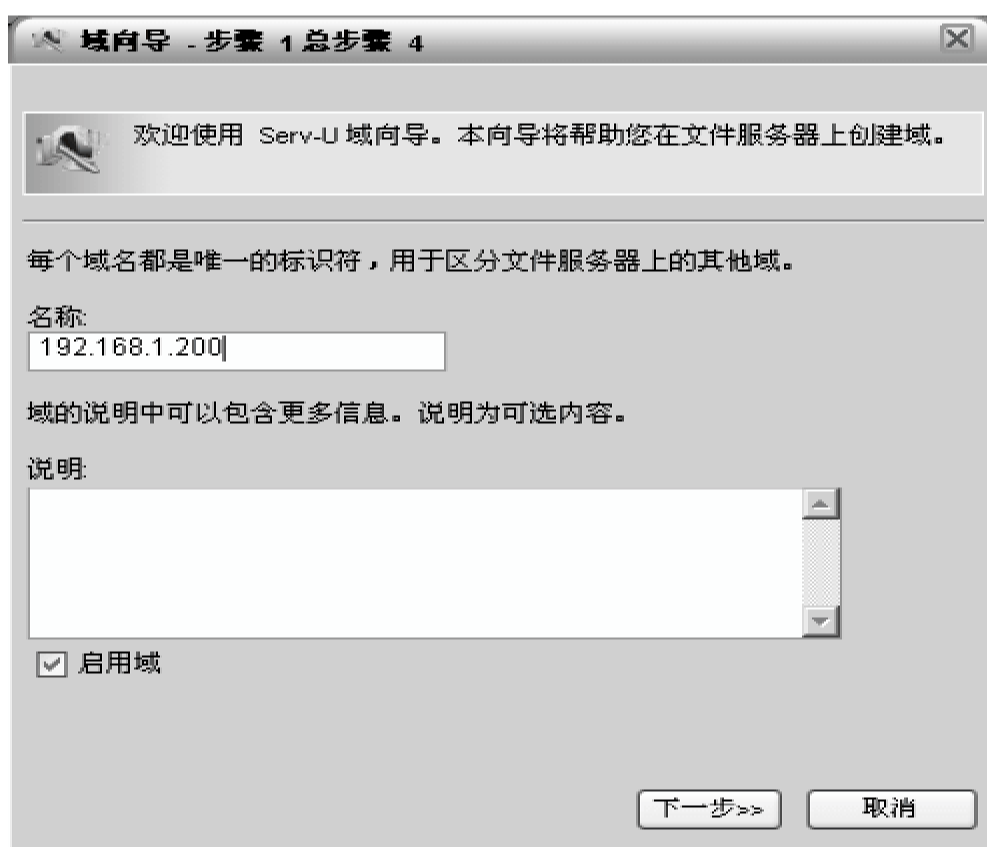


图 7-14 【域向导 – 步骤 1 总步骤 4】对话框

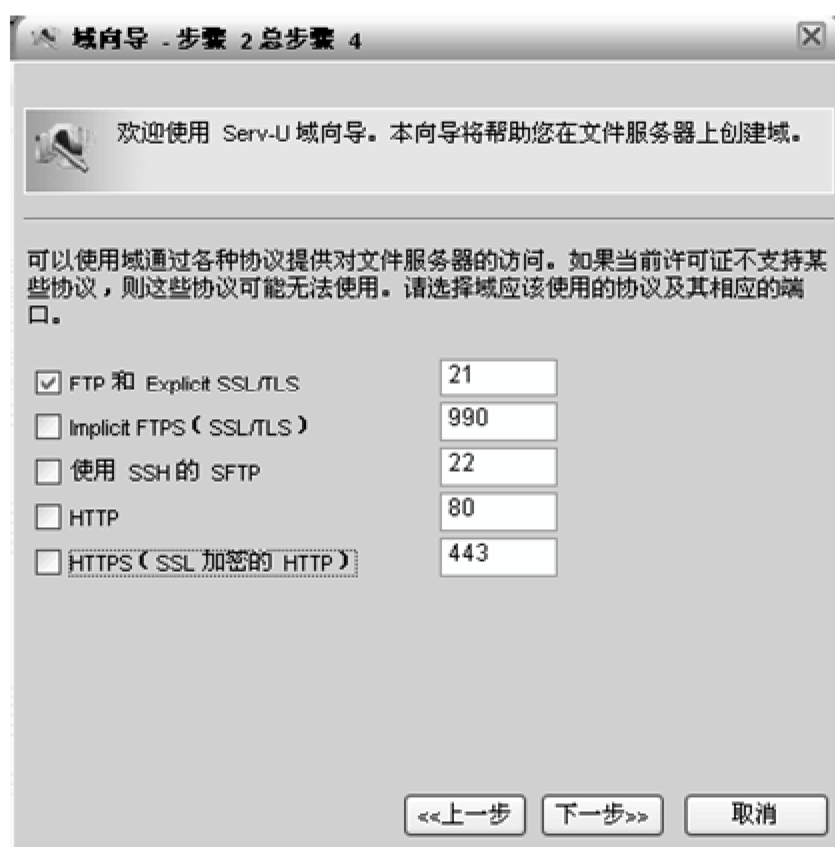


图 7-15 【域向导 – 步骤 2 总步骤 4】对话框

05 弹出【域向导 – 步骤 3 总步骤 4】对话框，在【IPv4 地址】下拉列表中选择需要使用的 IP 地址，本实例选择 IP 地址为“192.168.1.200”，也就是访问 FTP 服务器使用的 IP 地址，如图 7-16 所示，单击【下一步】按钮。

06 弹出【域向导 – 步骤 4 总步骤 4】对话框，选中【使用服务器设置（加密：单向加密）】单选按钮，如图 7-17 所示，单击【完成】按钮。

07 弹出【Serv-U】提示框，提示目前域中没有用户，如图 7-18 所示，单击【是】按钮，新建域中第一个用户。

08 在新弹出的提示框中，提示是否使用向导创建用户，如图 7-19 所示，单击【是】按钮。

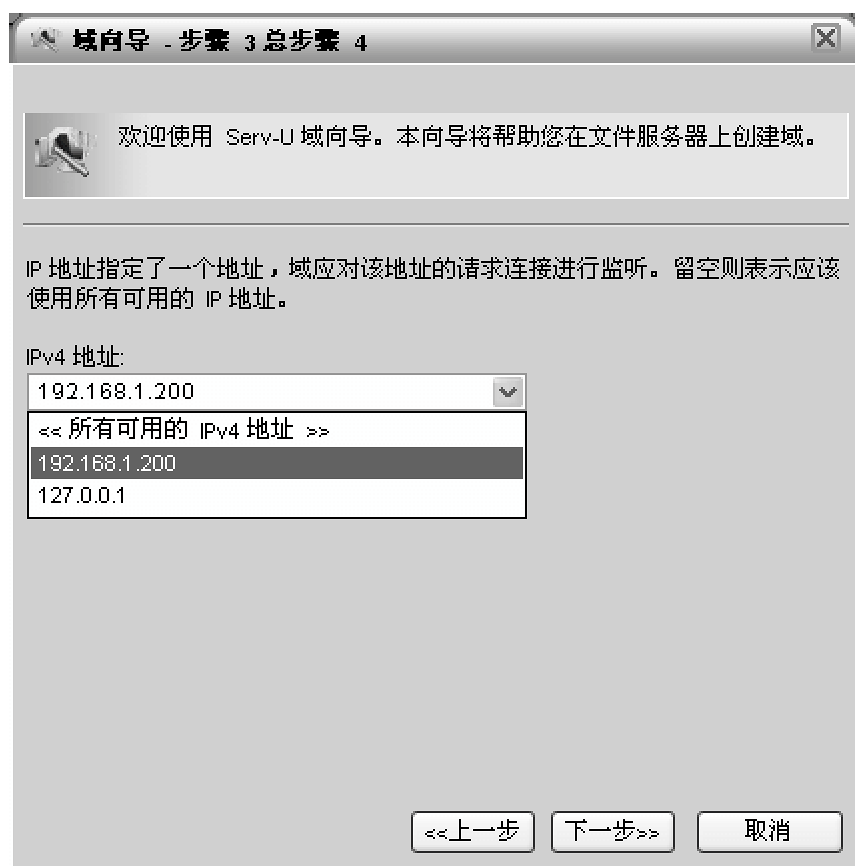


图 7-16　【域向导 – 步骤 3 总步骤 4】

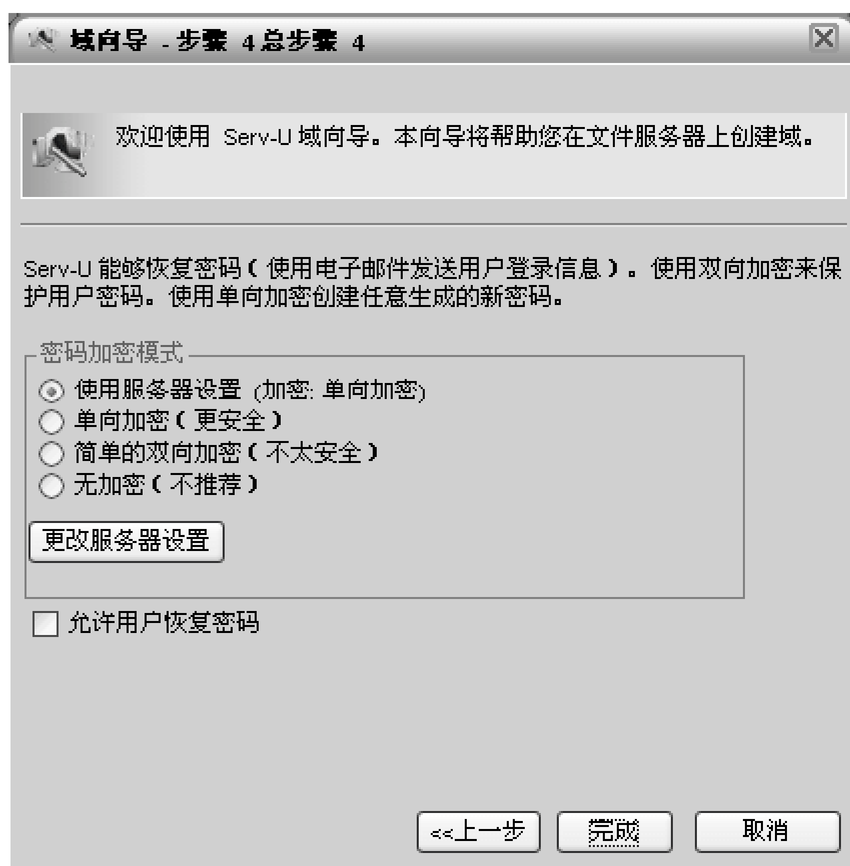


图 7-17　【域向导 – 步骤 4 总步骤 4】

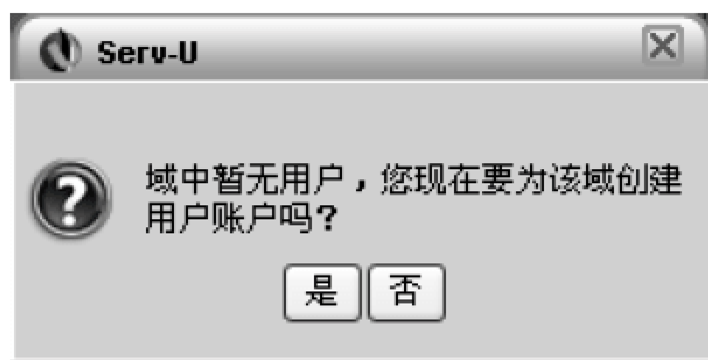


图 7-18　【Serv-U】提示框

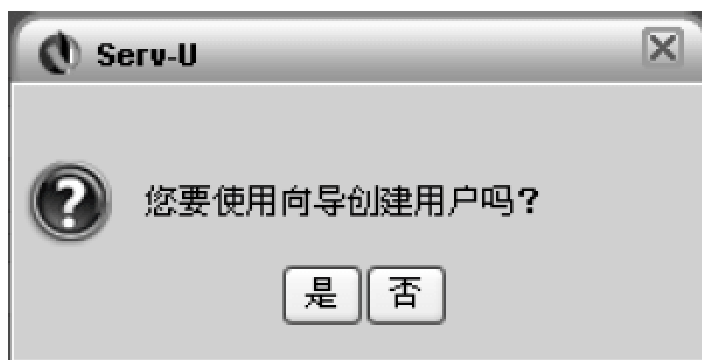


图 7-19　使用向导创建用户提示

09 弹出【用户向导 – 步骤 1 总步骤 4】对话框，在【登录 ID】文本框中输入账户名，本实例中输入的账户名为“anonymous”，表示为匿名用户登录，如图 7-20 所示，单击【下一步】按钮。

10 弹出【用户向导 – 步骤 2 总步骤 4】对话框，在【密码】文本框中输入匿名账户“anonymous”的密码，本实例中匿名账户密码为空，表明使用匿名账户登录时不需要输入密码，如图 7-21 所示，单击【下一步】按钮。

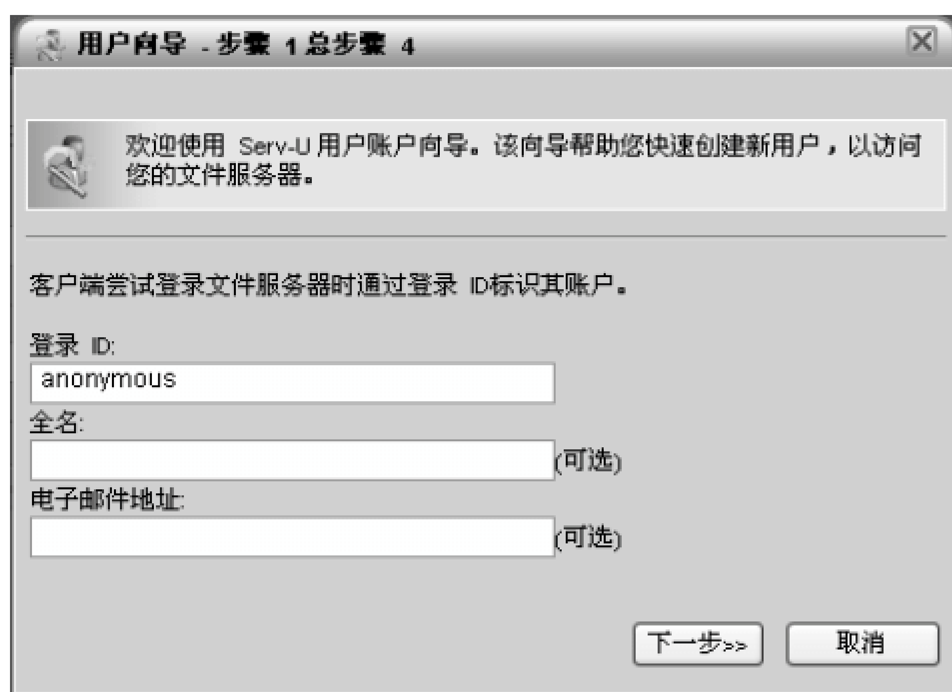


图 7-20　【用户向导 – 步骤 1 总步骤 4】对话框

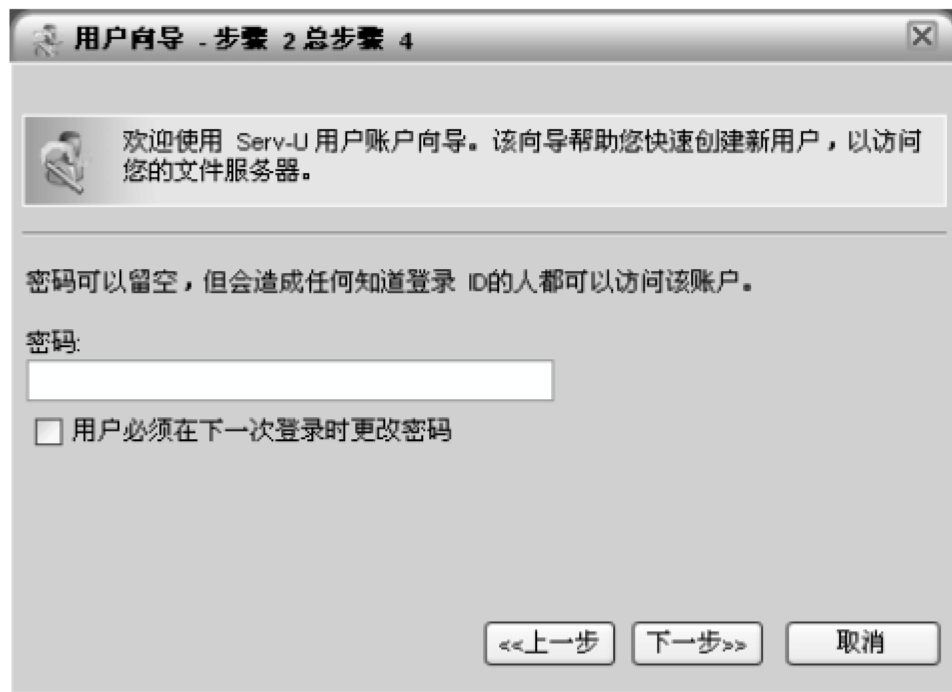


图 7-21　【用户向导 – 步骤 2 总步骤 4】对话框

11 弹出【用户向导 – 步骤 3 总步骤 4】对话框，选中【锁定用户至根目录】复选框，如图 7-22 所示，单击【根目录】文本框后面的图标。

12 弹出【浏览】对话框，在【目录路径】文本框中输入匿名账户“anonymous”访问的根目录，本实例中匿名账户访问的根目录为“C:/FTP/public”，如图 7-23 所示，单击【选择】按钮。

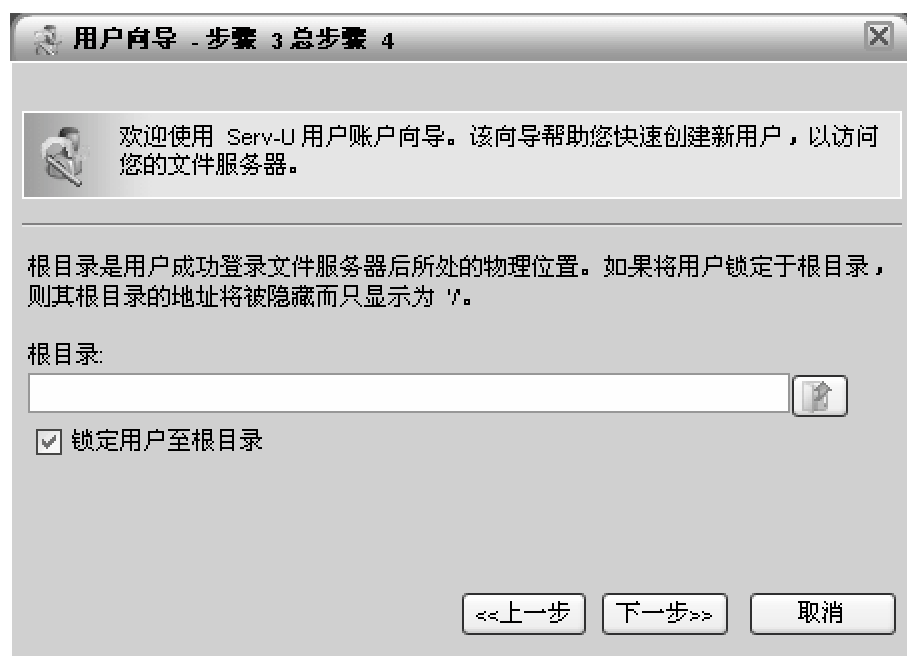


图 7-22 【用户向导 – 步骤 3 总步骤 4】对话框

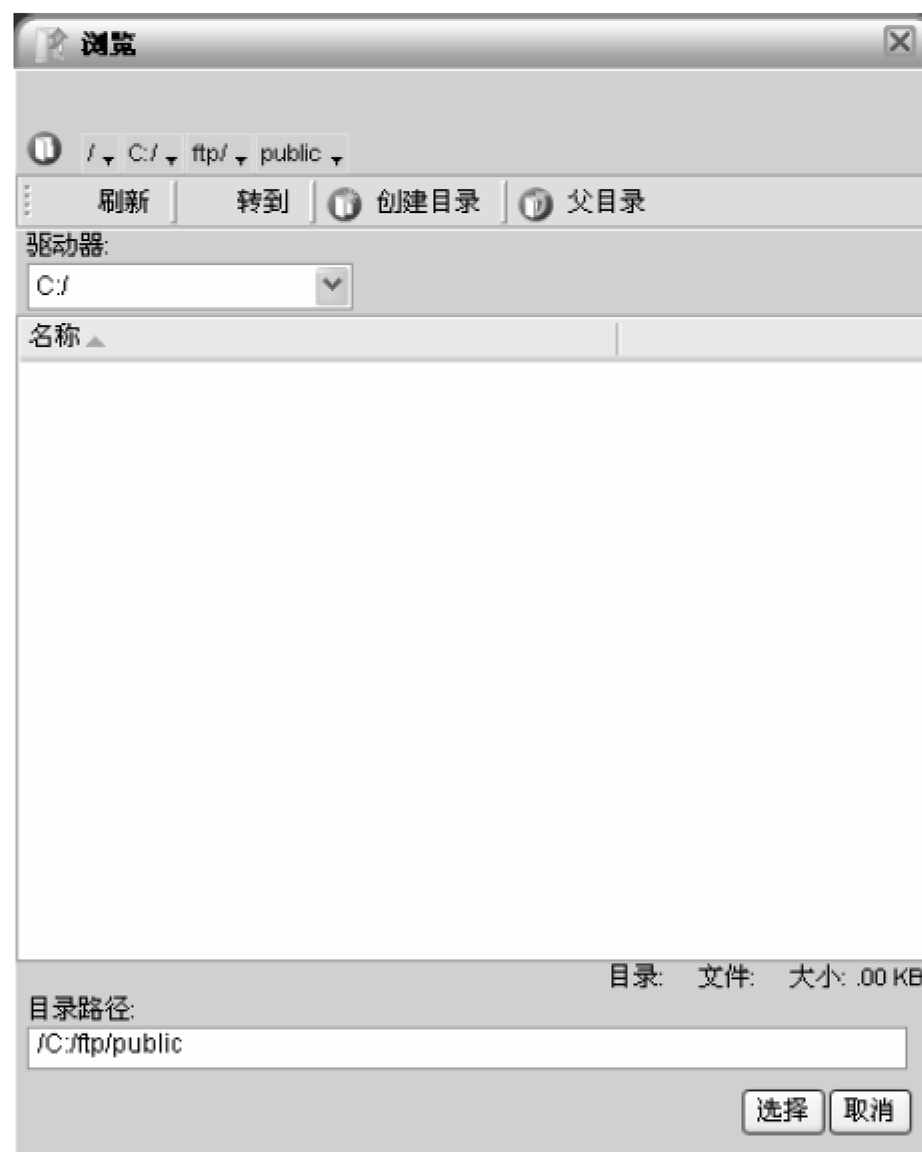


图 7-23 【浏览】对话框

13 返回至【用户向导 – 步骤 3 总步骤 4】对话框，如图 7-24 所示，单击【下一步】按钮。

14 弹出【用户向导 – 步骤 4 总步骤 4】对话框，在【访问权限】下拉列表中选择【只读访问】选项，如图 7-25 所示，单击【完成】按钮。

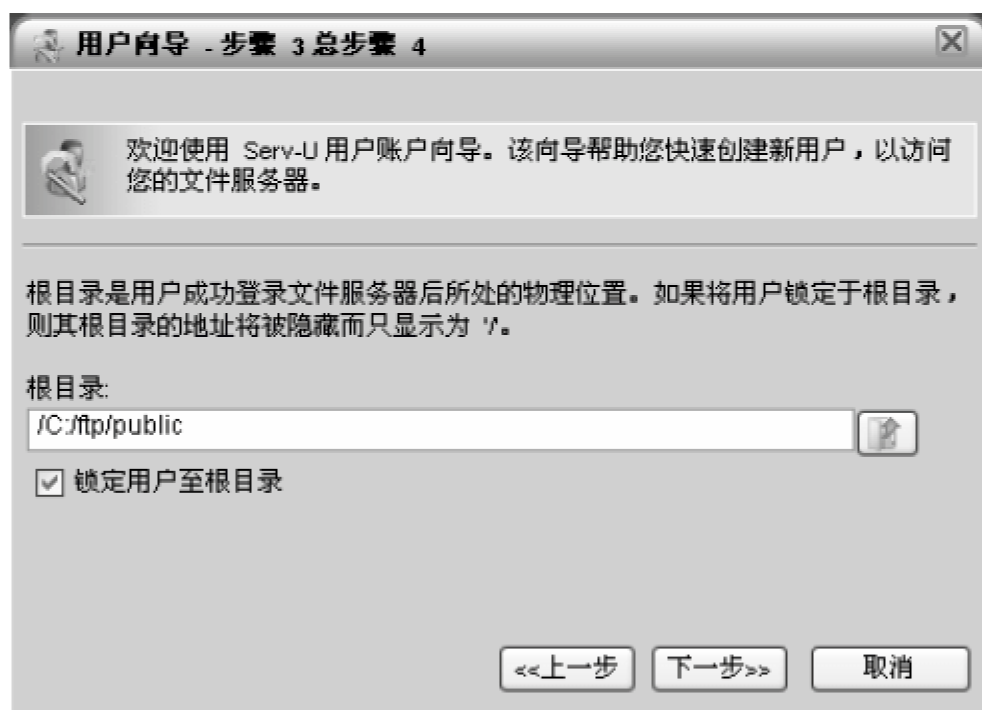


图 7-24 【用户向导 – 步骤 3 总步骤 4】对话框

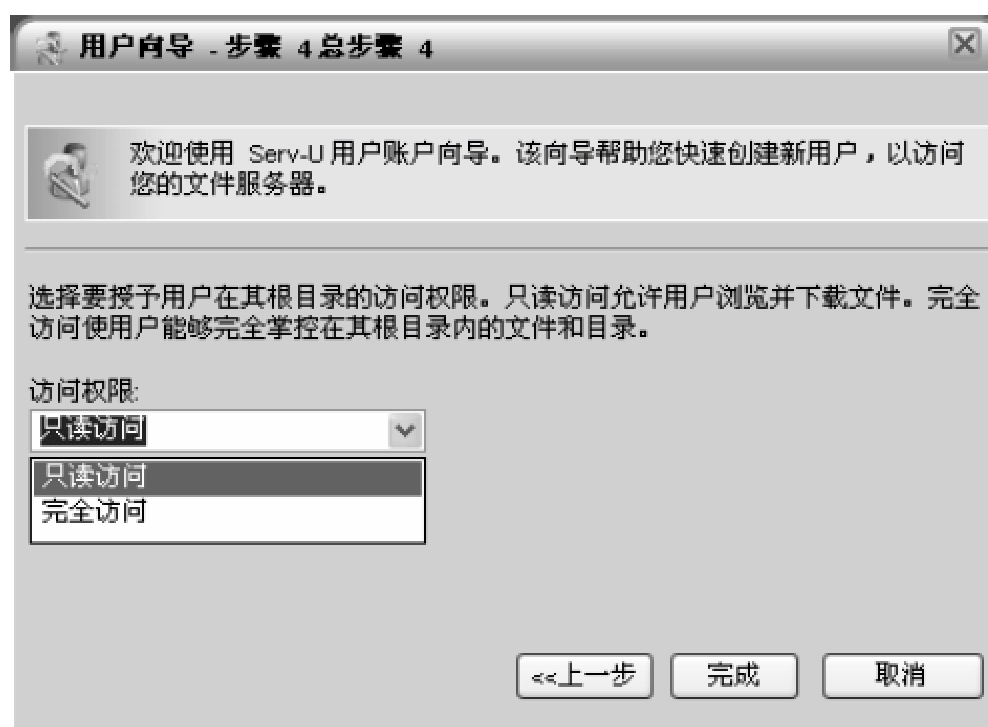


图 7-25 【用户向导 – 步骤 4 总步骤 4】对话框

15 返回至【Serv-U 管理控制台 – 用户】操作界面，如图 7-26 所示，至此 Serv-U 匿名用户创建完毕。

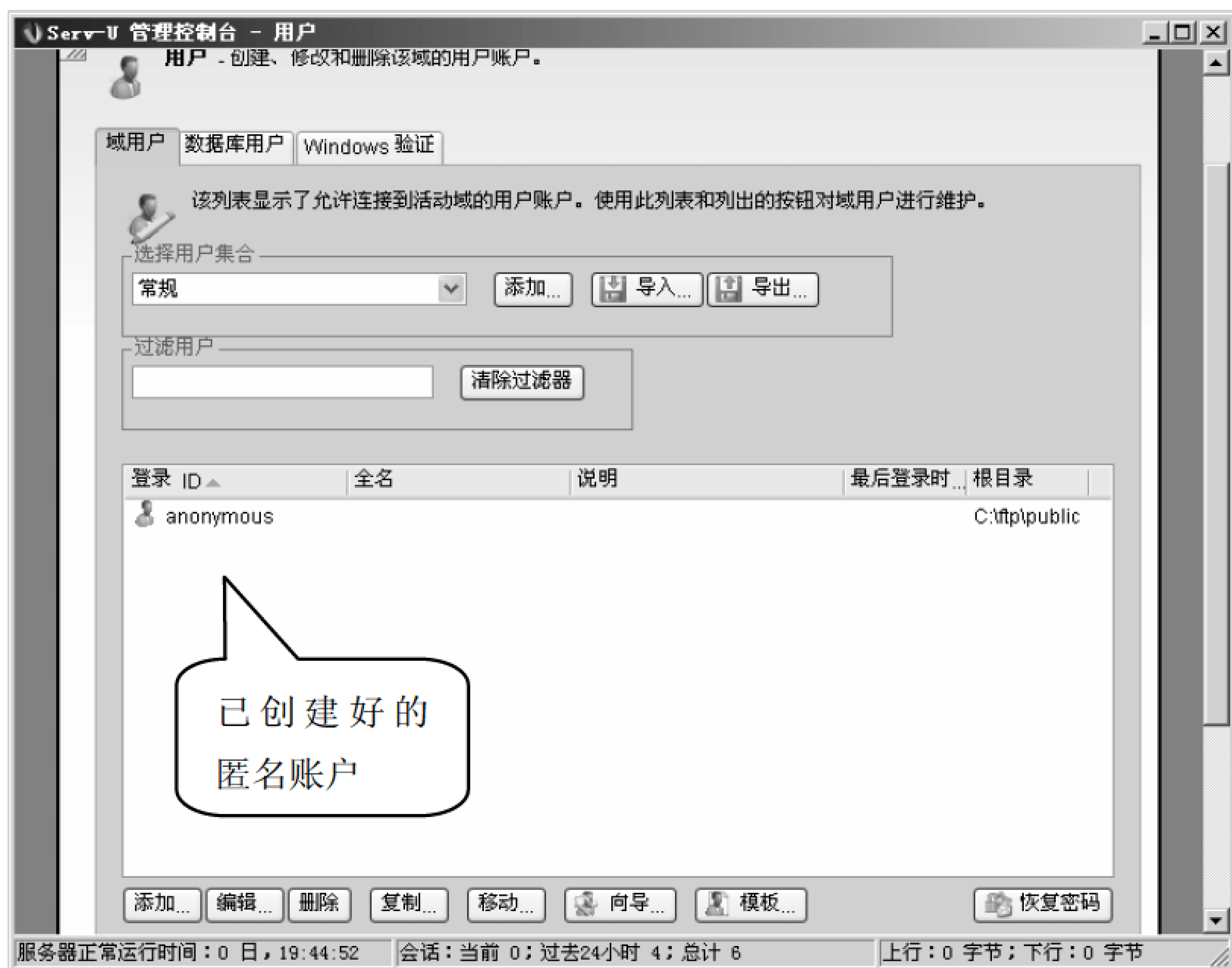


图 7-26　【Serv-U 管理控制台 － 用户】界面

2. 为员工苏红添加账户

为员工苏红添加账户，账户名为“sh”，密码为“123”。要求苏红对自己的根目录有读取和写入权限，但是不能删除目录中的内容，同时苏红只能使用 FTP 服务器 500MB 硬盘空间。

依照上面的要求为员工苏红添加账户，具体操作步骤如下。

01 双击桌面上 Serv-U 快捷方式，弹出【已启用 Windows Internet 增强的安全配置】提示框，选中【不要再显示此提示】复选框，如图 7-27 所示，单击【确定】按钮。

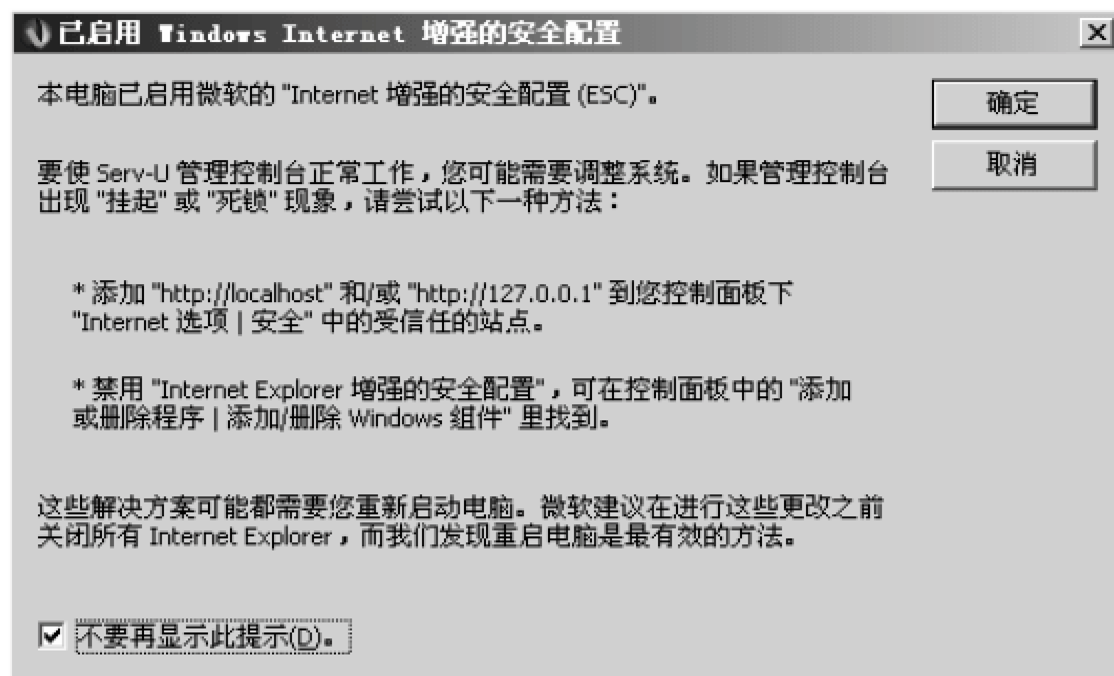


图 7-27　【已启用 Windows Internet 增强的安全配置】提示框

02 弹出【Serv-U 管理控制台 － 主页】窗口，单击【用户】一栏中的【创建、修改和删除用户账号】链接，如图 7-28 所示。

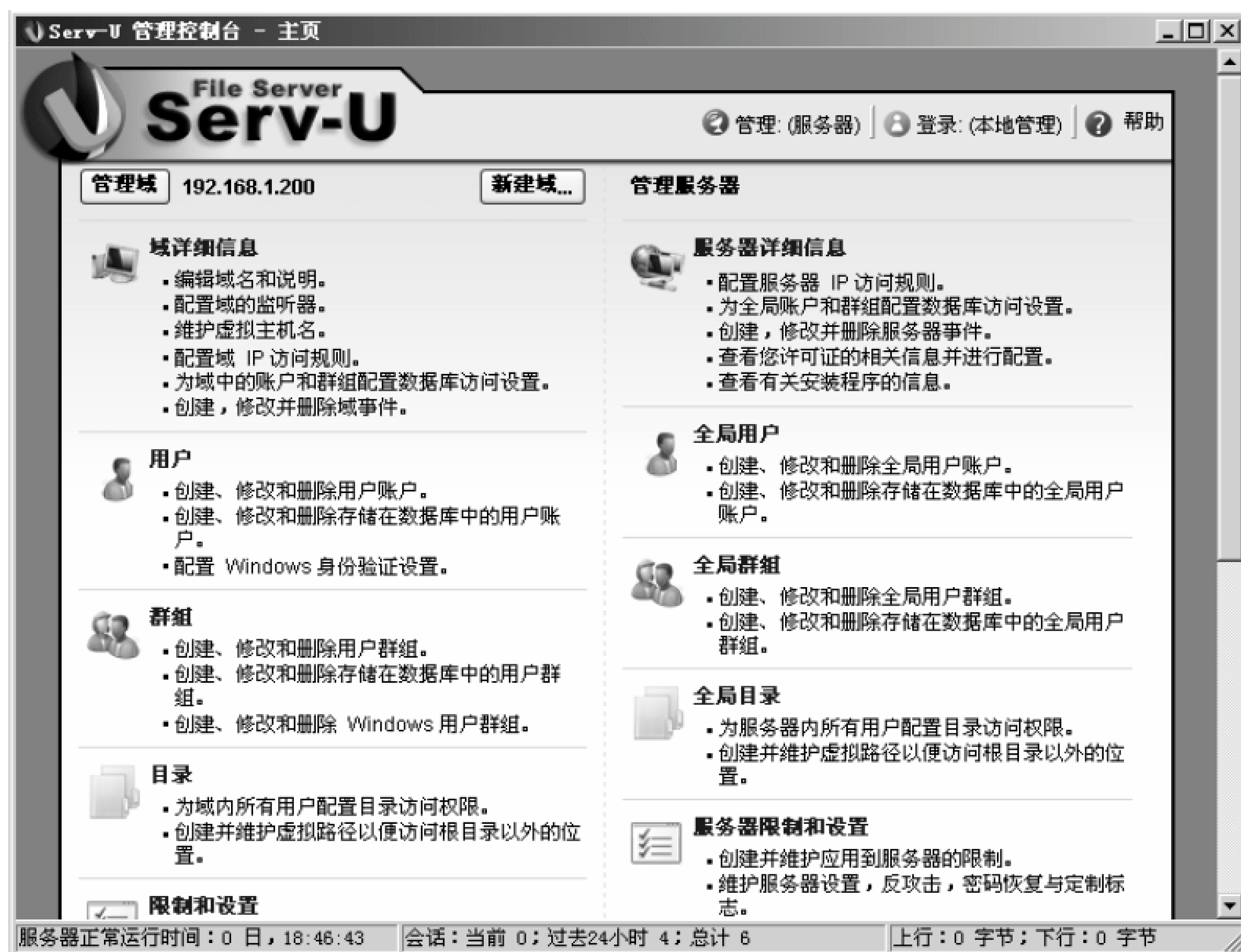


图 7-28 【Serv-U 管理控制台 – 主页】窗口

03 弹出【Serv-U 管理控制台 – 用户】窗口，单击【添加】按钮。

04 弹出【用户属性 – sh】对话框，在【登录 ID】文本框中输入员工苏红的账户“sh”，在【密码】文本框中输入密码为“123”，单击【根目录】文本框后面的图标，如图 7-29 所示。



图 7-29 【用户属性 – sh】对话框

05 弹出【浏览】对话框，在【目录路径】文本框中输入账户 sh 访问的根目录，本实例输入根目录路径为“C:/ftp/yuangong/sh”，单击【选择】按钮，如图 7-30 所示。

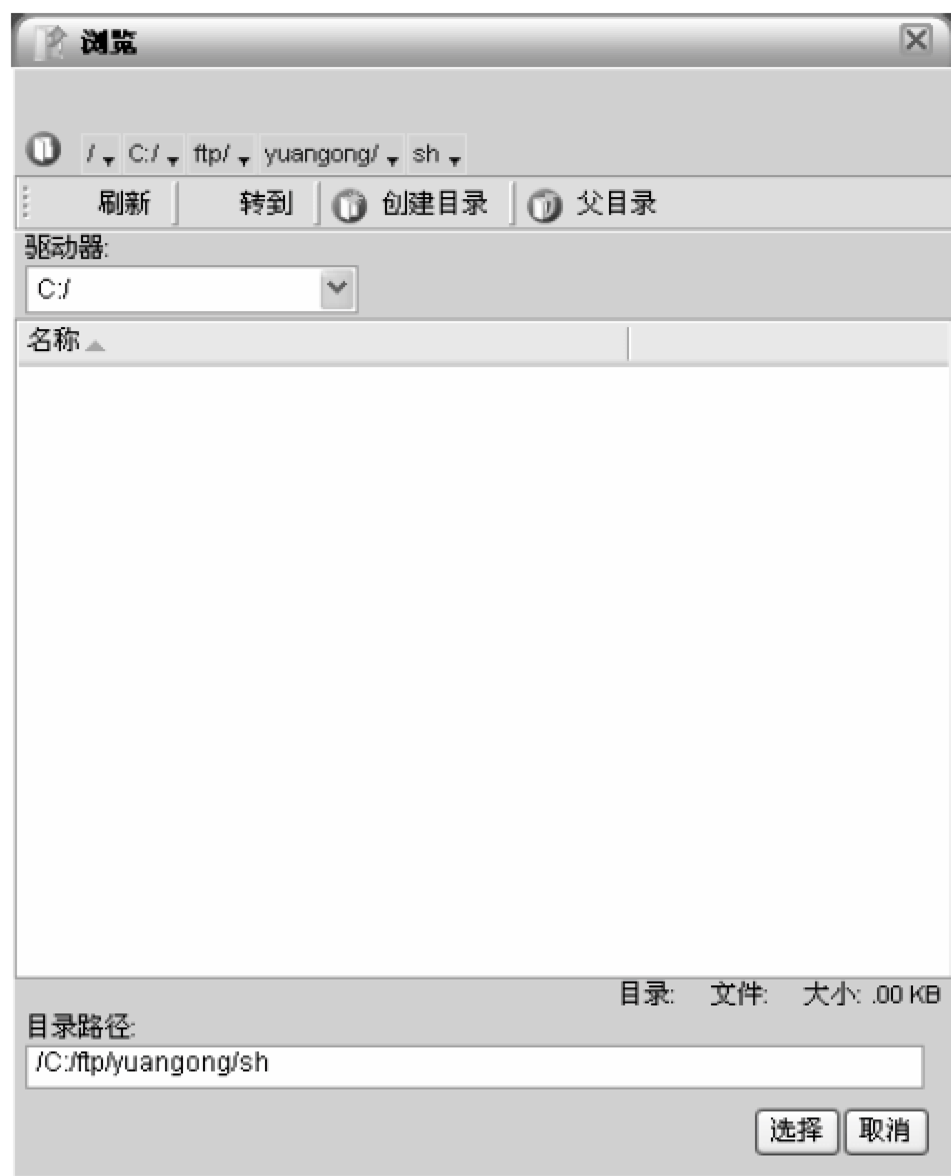


图 7-30　【浏览】对话框

06 返回至【用户属性】对话框，如图 7-31 所示，选择【目录访问】选项卡，单击【添加】按钮。

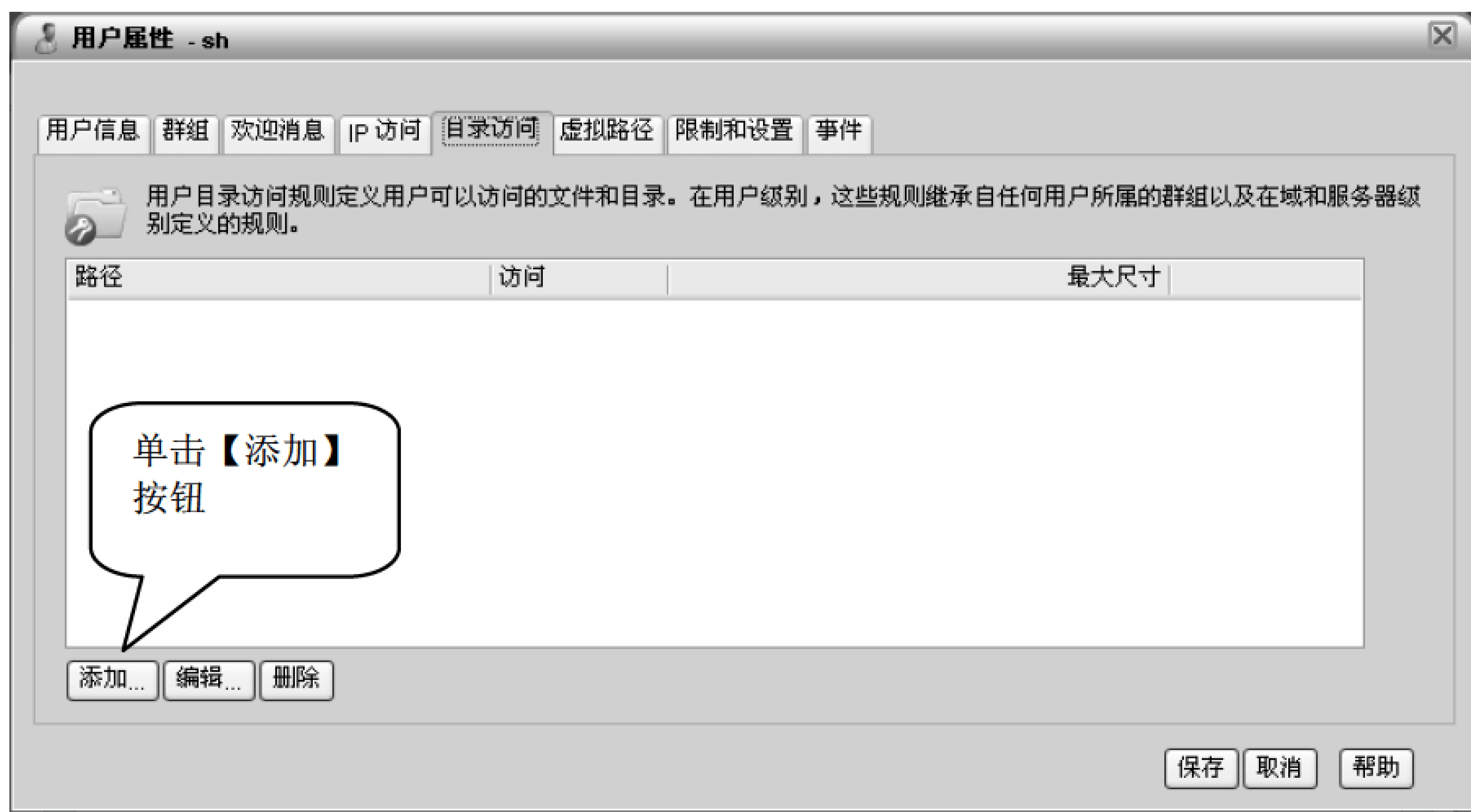


图 7-31　【用户属性】对话框

07 弹出【目录访问规则】对话框，如图 7-32 所示，单击【路径】文本框后面的图标。

08 弹出【浏览】对话框，在【目录路径】文本框中输入账户“sh”的根目录路径，本实例为“C:/ftp/yuangong/sh”，如图 7-33 所示，单击【选择】按钮。

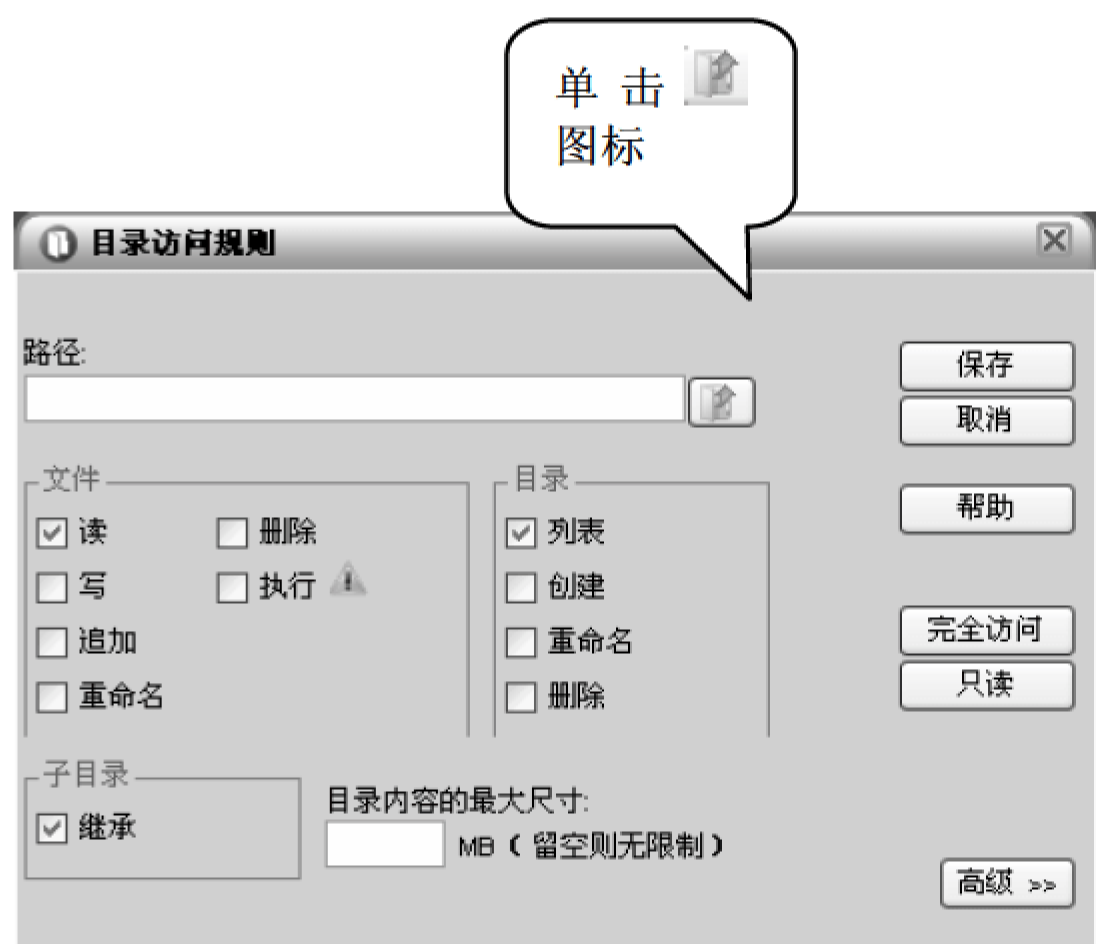


图 7-32 【目录访问规则】对话框



图 7-33 【浏览】对话框

09 返回至【目录访问规则】对话框，选中【读】、【写】、【继承】、【创建】和【列表】复选框，在【目录内容的最大尺寸】文本框中输入“500”，表示账户 sh 可以使用 FTP 服务器的硬盘空间大小为“500MB”，如图 7-34 所示，单击【保存】按钮。

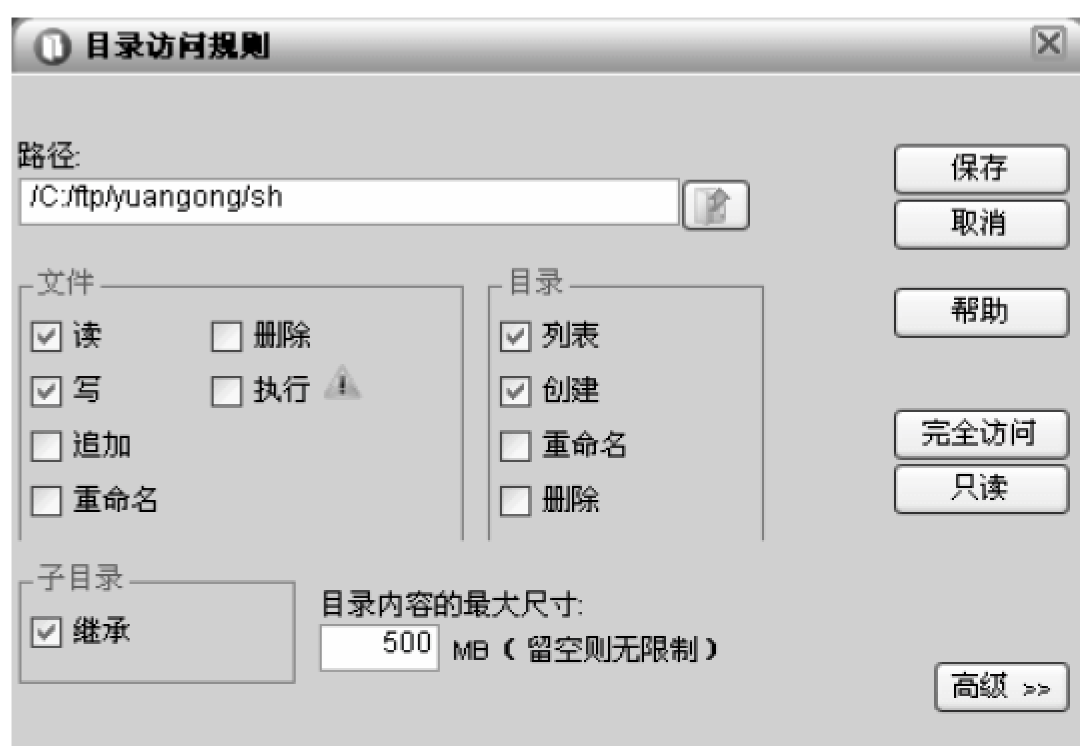


图 7-34 【目录访问规则】对话框

10 返回至【用户属性 – sh】对话框的【目录访问】选项卡，如图 7-35 所示，单击【保存】按钮。

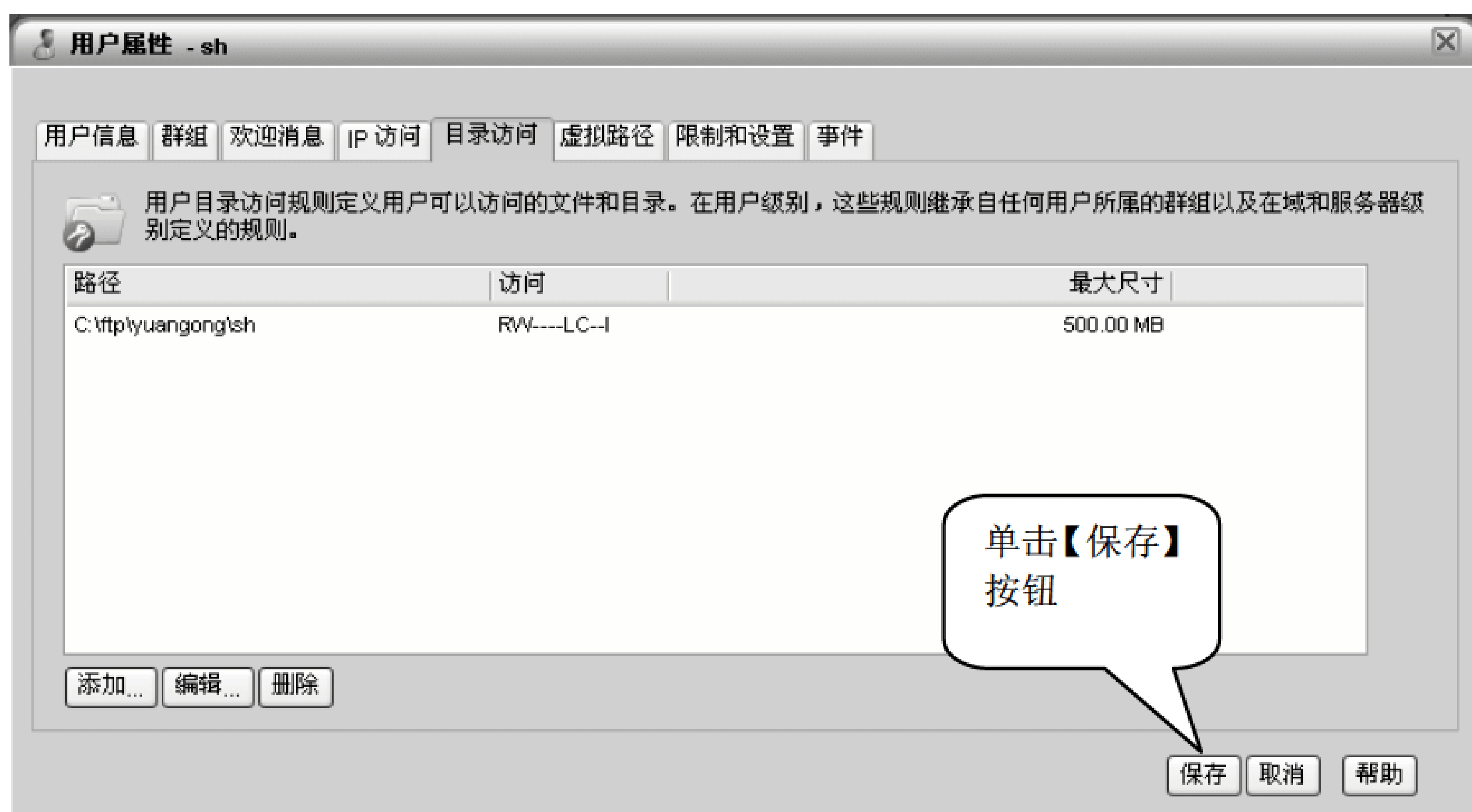


图 7-35　【目录访问】选项卡

11 返回至【Serv-U 管理控制台 – 用户】对话框，如图 7-36 所示，单击【添加】按钮，继续添加新的员工账户。

12 弹出【用户属性】对话框，在【登录 ID】和【密码】文本框中分别输入登录账户和密码，本实例中员工王明创建的 FTP 账户，用户名为“wm”，密码为“123”，如图 7-37 所示。单击【根目录】文本框后面的 图标。

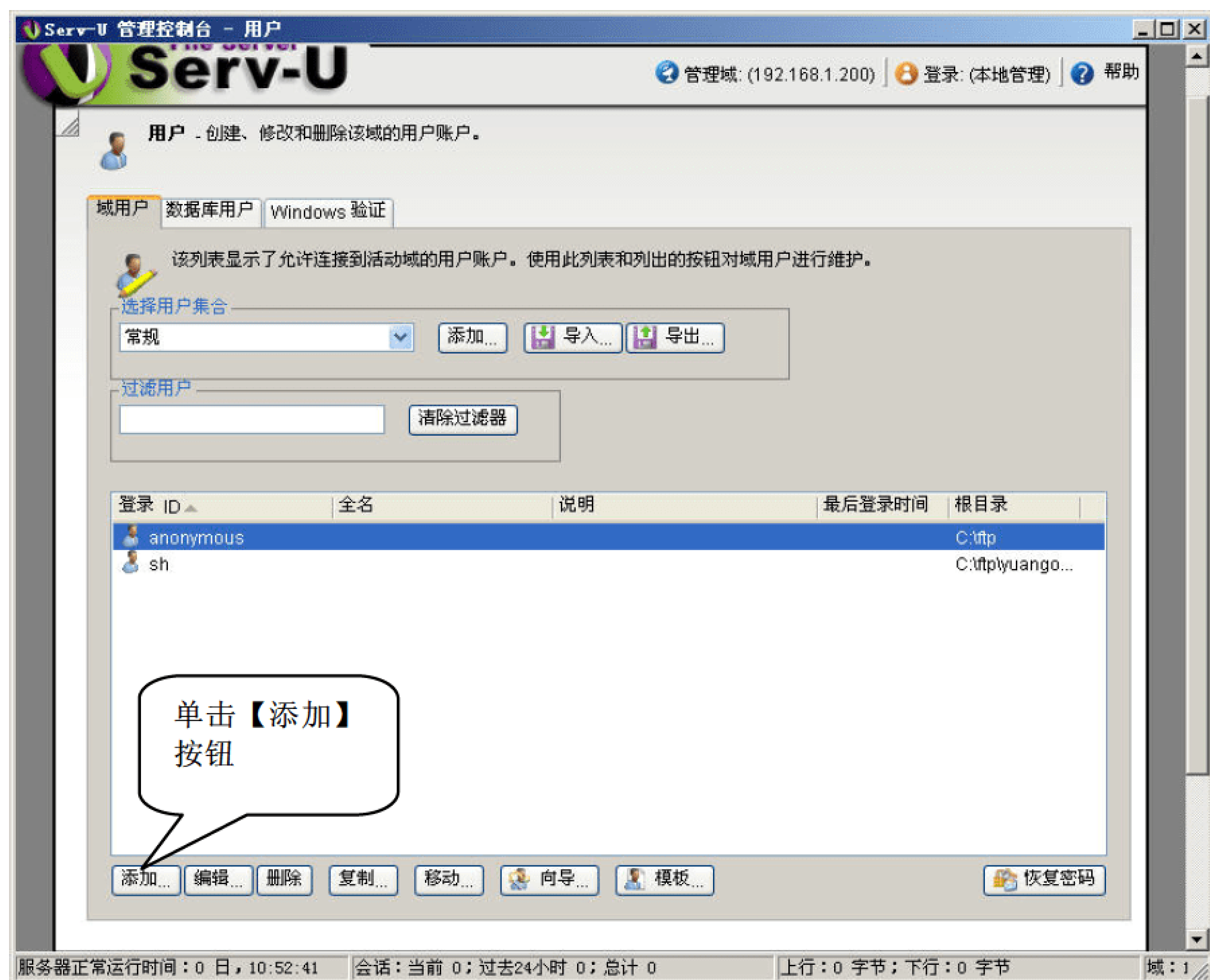


图 7-36　【Serv-U 管理控制台 – 用户】对话框

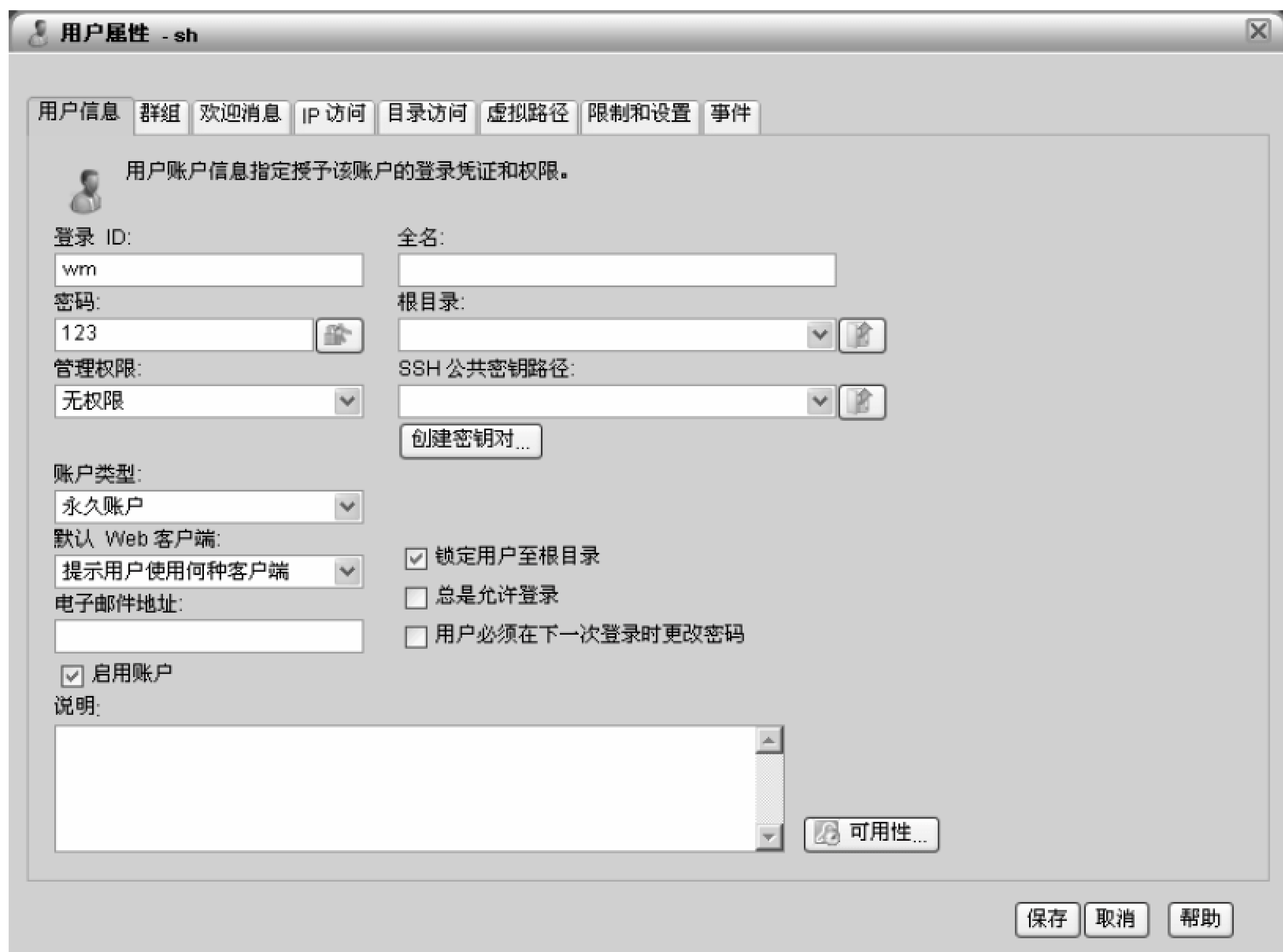


图 7-37 【用户属性】对话框

13 弹出【浏览】对话框，在【目录路径】文本框中输入账户“wm”访问的根目录的路径，本实例中输入账户“wm”访问的根目录的路径为“C:/ftp/yuangong/wm”，如图 7-38 所示，单击【选择】按钮。

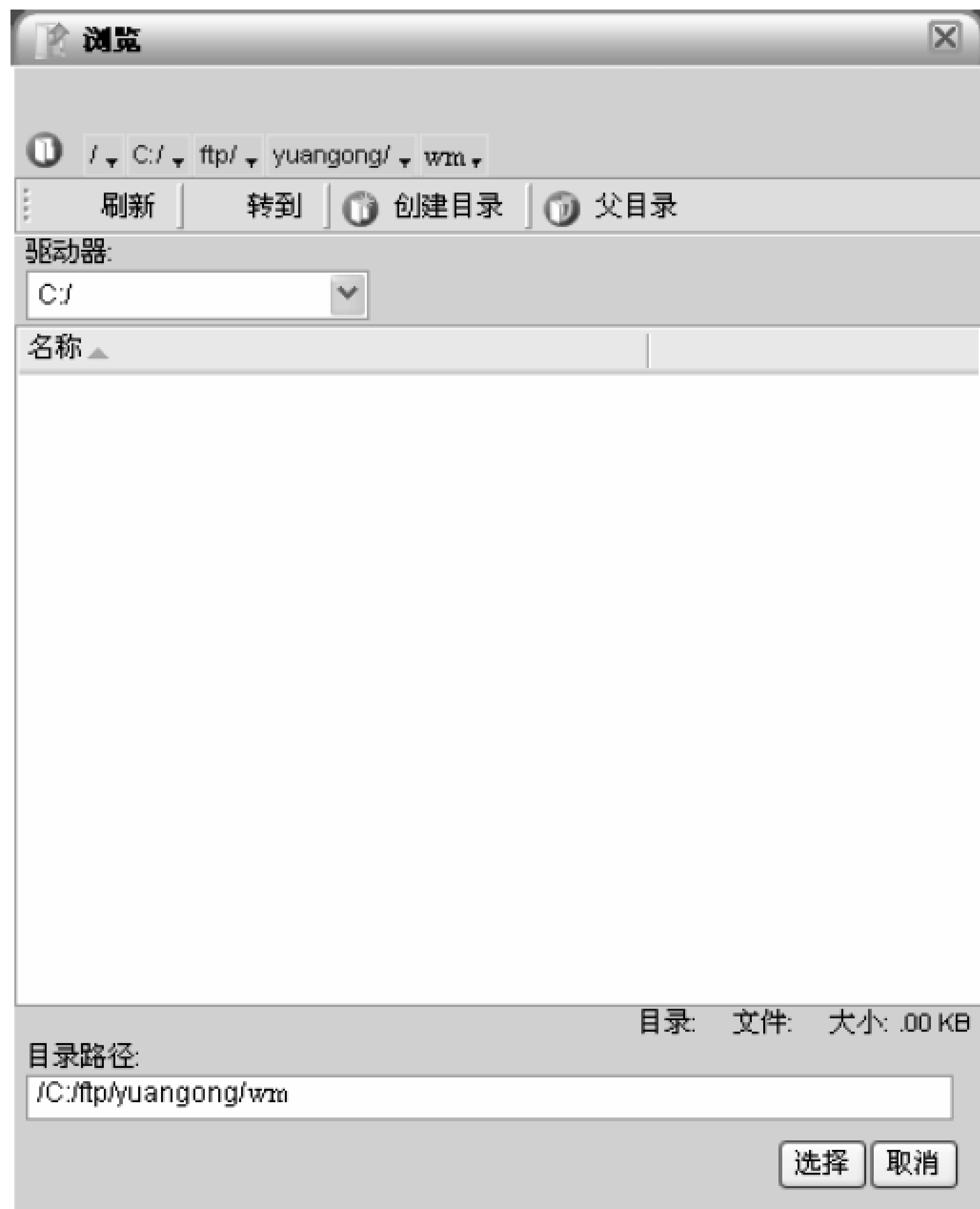


图 7-38 【浏览】对话框

14 返回【用户属性 – wm】对话框，选择【目录访问】选项卡，如图 7-39 所示，单击【添加】按钮。



图 7-39 【用户属性 – wm】目录访问对话框

15 打开【目录访问规则】对话框，选中【文件】选项组中【读】、【写】和【删除】复选框，选中【目录】选项组中【列表】、【创建】、【重命名】和【删除】复选框，权限设置完成。在【目录内容的最大尺寸】文本框中输入“500”，表示账户“wm”可以使用 FTP 硬盘空间“500MB”，如图 7-40 所示，单击【路径】文本框后面的 图标。

16 弹出【浏览】对话框，在【目录路径】文本框中输入账户“wm”访问的根目录，本实例中账户“wm”的根目录为“C:/ftp/yuangong/wm”，如图 7-41 所示，单击【选择】按钮。

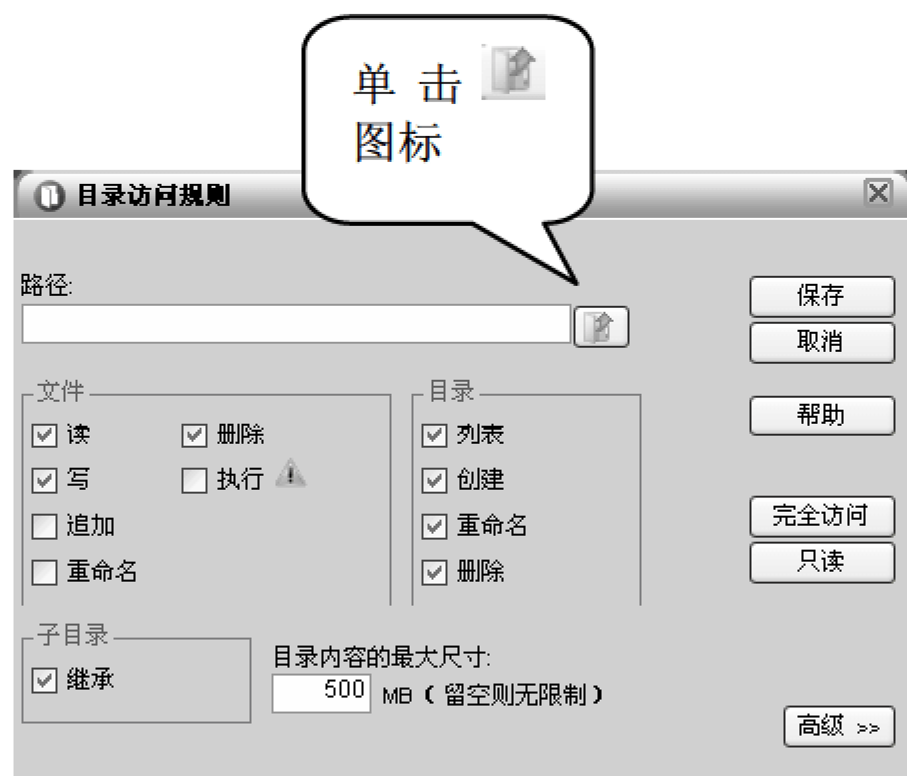


图 7-40 【目录访问规则】对话框

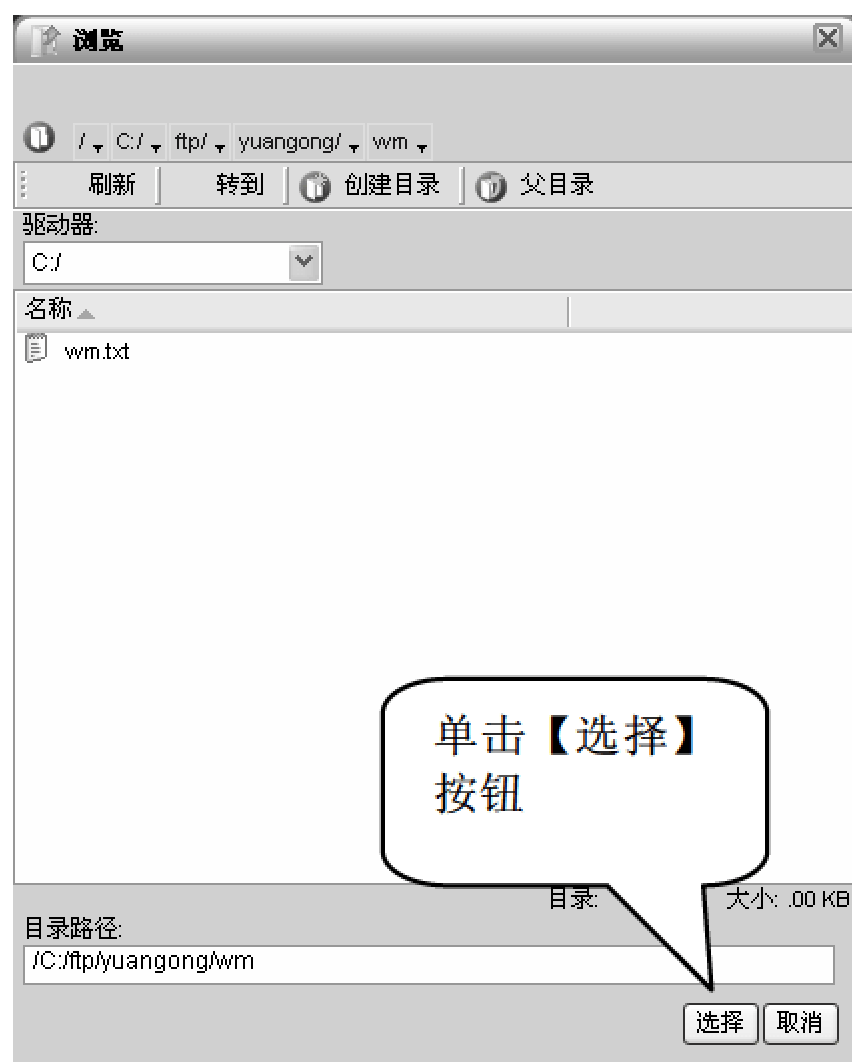


图 7-41 【浏览】对话框

17 返回至【目录访问规则】对话框，如图 7-42 所示，单击【保存】按钮。

18 返回至【用户属性 – wm】对话框，如图 7-43 所示，单击【保存】按钮。

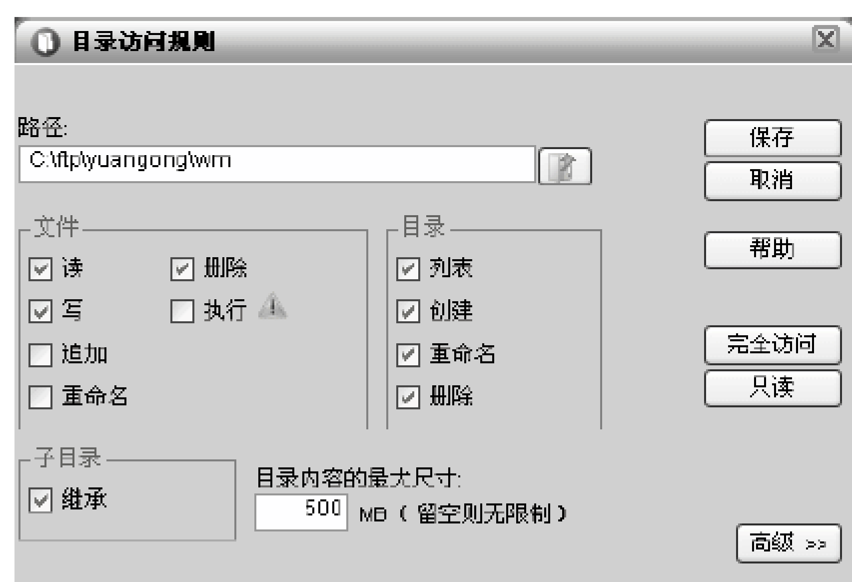


图 7-42 【目录访问规则】对话框



图 7-43 【用户属性 – wm】对话框

19 返回至【Serv-U 管理控制台 – 用户】对话框，如图 7-44 所示，照此流程添加经理账户 wxl，在此不再赘述。



图 7-44 【Serv-U 管理控制台 – 用户】对话框

3. 客户端访问

在网络中的一台 PC 上访问 FTP 服务器的具体操作步骤如下。

01 双击桌面上【我的计算机】图标，在地址栏里输入“ftp://192.168.1.200”，其中“192.168.1.200”为 FTP 服务器的 IP 地址，如图 7-45 所示，按下【Enter】键确认，打开匿名用户成功登录 FTP 服务器的界面。

02 在空白处右击，在弹出的快捷菜单中选择【登录】命令，如图 7-46 所示。



图 7-45　匿名登录 FTP



图 7-46　登录 FTP

03 弹出【登录身份】对话框，在【用户名】和【密码】文本框中输入合法的账户和密码，本实例中输入经理账户为“wxl”，密码为“123”，单击【登录】按钮，如图 7-47 所示。

04 返回至 FTP 服务登录窗口，如图 7-48 所示，可以看到经理王晓亮使用账户 wxl 已经成功登录，并可以看到自己主目录的内容。

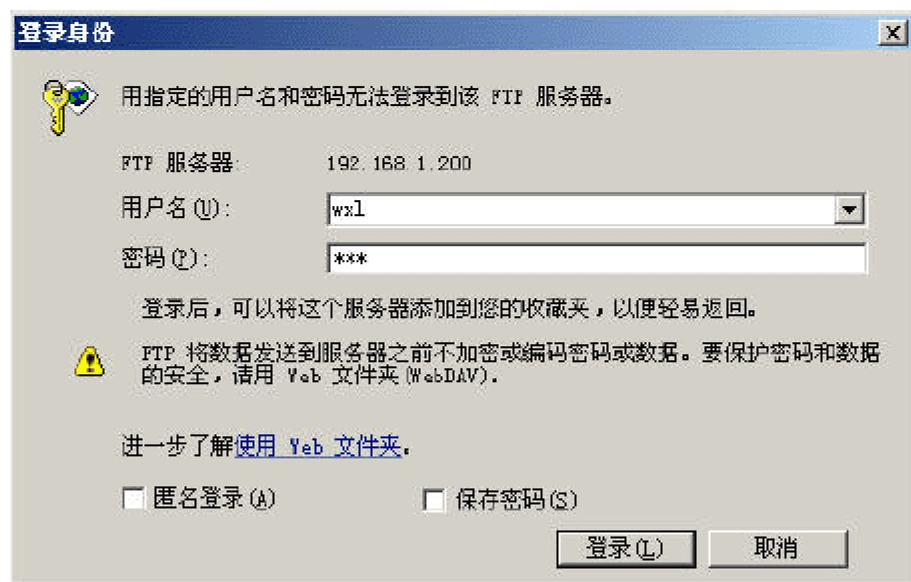


图 7-47　【登录身份】对话框



图 7-48　FTP 服务登录窗口

7.2.3　实现同一账户在多网段访问具有不同权限

很多时候为了安全的需要，或者是管理的方便，在 FTP 服务器上安装两块网卡，这样的话可以在 Serv-U 服务器上建立两个域，如图 7-49 所示，不同的域使用不同的 IP 地址，每个域可以有独立的账户密码，实现同一账户访问不同的域，使用不同的密码具有不同的权限的情况。下面详细介绍如何在 Serv-U 软件上通过建立不同的域来实现同一账户在多网段访问具有不同的权限。



图 7-49 【网络连接】窗口

1. 实现同一账户在多网段访问具有不同的权限

要想实现同一账户在多网段访问具有不同的权限，需要在 Serv-U 服务器上建立多个 FTP 域。建立 Serv-U 域的具体操作步骤如下。

01 双击桌面上 Serv-U 图标，显示【已启用 Windows Internet 增强的安全配置】提示框，选中【不要再显示此提示】复选框，如图 7-27 所示，单击【确定】按钮。

02 打开 Serv-U 的管理控制台操作界面，如图 7-28 所示，单击【新建域】按钮。

03 弹出【域向导 – 步骤 1 总步骤 4】对话框，在【名称】文本框中输入域的名称，本实例输入域的名称为“172.16.1.200”，选中【启用域】复选框，如 7-50 所示，单击【下一步】按钮。

04 弹出【域向导 – 步骤 2 总步骤 4】对话框，选中【FTP 和 Explicit SSL/TLS】复选框，如图 7-15 所示，单击【下一步】按钮。



图 7-50 【域向导 – 步骤 1 总步骤 4】对话框

05 弹出【域向导 – 步骤 3 总步骤 4】对话框，在【IPv4 地址】下拉列表中选择 IP 地址为“172.16.1.200”，表明以后访问该 FTP 服务器的这个域使用 IP 地址“172.16.1.200”。注意本域的地址应该和上文中创建的域使用的 IP 地址不同，如图 7-51 所示，单击【下一步】按钮。

06 弹出【域向导 – 步骤 4 总步骤 4】对话框，如图 7-17 所示，选中【使用服务器设置（加密：单向加密）】复选框，单击【完成】按钮。



图 7-51　【域向导 – 步骤 3 总步骤 4】对话框

07 弹出【Serv-U】提示框，提示域中没有用户，是否要为该域创建账户，如图 7-18 所示，单击【是】按钮。

08 弹出【使用向导创建用户】创建用户向导对话框，如图 7-19 所示，单击【是】按钮。

09 弹出【用户向导 – 步骤 1 总步骤 4】对话框，在【登录 ID】文本框中输入账户，本实例中输入匿名账户“anonymous”，如图 7-20 所示，单击【下一步】按钮。

10 弹出【用户向导 – 步骤 2 总步骤 4】对话框，清空【密码】对话框中的数据，意味着匿名账户“anonymous”密码为空，如图 7-21 示，单击【下一步】按钮。

11 弹出【用户向导 – 步骤 3 总步骤 4】对话框，如图 7-22 所示，单击【根目录】文本框后面的 图标。

12 弹出【浏览】对话框，在【目录路径】文本框中输入匿名账户 anonymous 访问的根目录路径，本实例中匿名账户访问的根目录的路径为 C:/ftp/public，如图 7-22 所示，单击【选择】按钮。

13 返回【用户向导 – 步骤 3 总步骤 4】对话框，选中【锁定用户至根目录】复选框，如图 7-24 所示，单击【下一步】按钮。

14 弹出【用户向导 – 步骤 4 总步骤 4】对话框，在【访问权限】下拉列表中选择【只读访问】权限，如图 7-25 所示，单击【完成】按钮。

15 返回至【Serv-U 管理控制台 – 用户】对话框，如图 7-26 所示，单击【添加】按钮。

16 弹出【用户属性 – wm】对话框，在【登录 ID】和【密码】文本框中分别输入账户和密码，本实例输入员工王明的账户，账户名为“wm”，密码为“wm”，如图 7-52 所示，单击【根目录】文本框后面的 图标。

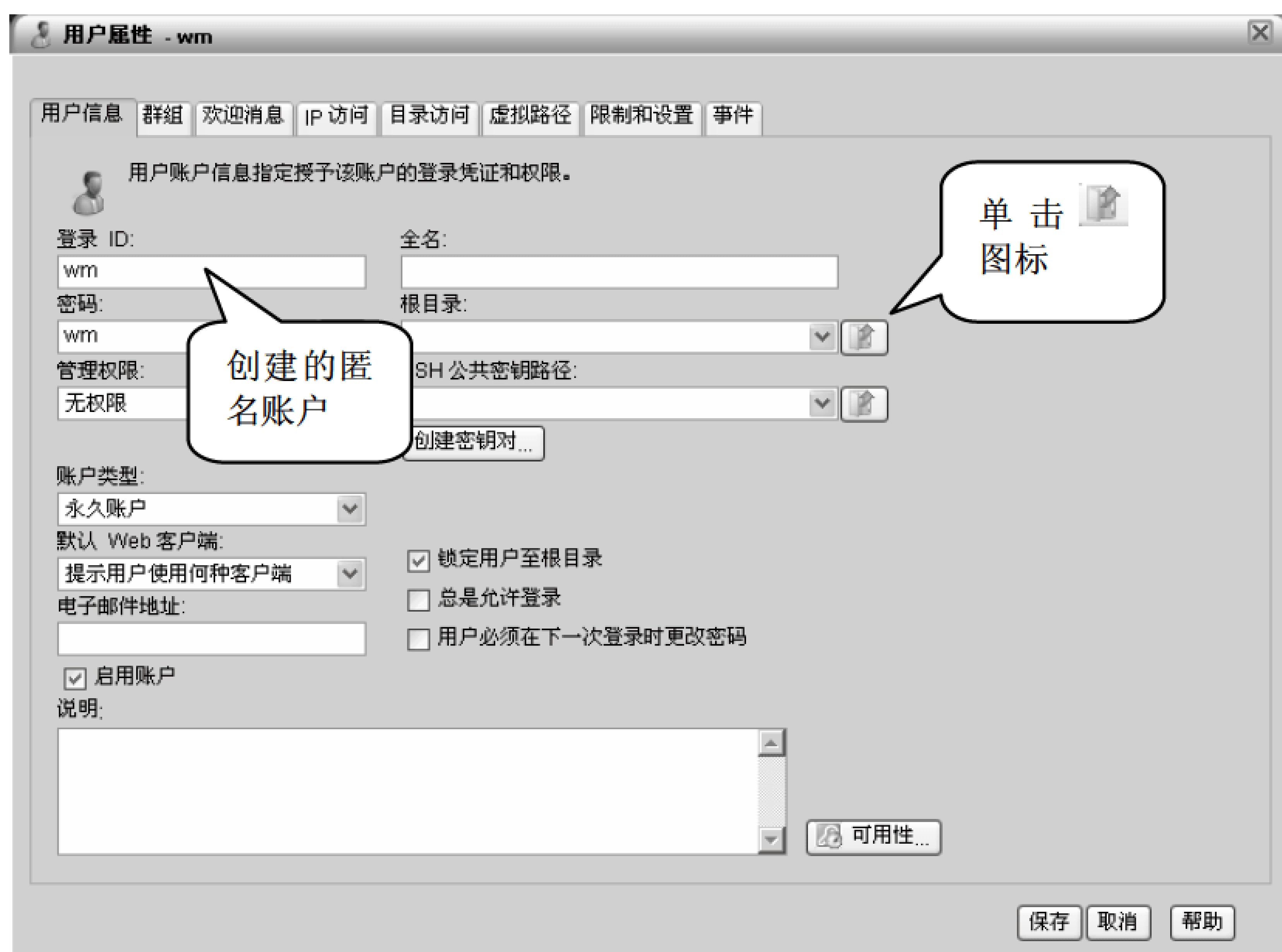


图 7-52 【用户属性 – wm】对话框

17 弹出【浏览】对话框，在【目录路径】文本框中输入员工王明访问的根目录路径，本实例中输入王明的根目录路径为“C:/ftp/yuangong/wm”，如图 7-38 所示，单击【选择】按钮。

18 返回至【用户属性 – wm】对话框，如图 7-39 所示，选择【目录访问】选项卡，单击【添加】按钮。

19 弹出【目录访问规则】对话框，选中【文件】选项组中的【读】和【目录】选项组中的【列表】复选框，单击【路径】文本框后面的图标，如图 7-53 所示。

20 弹出【浏览】对话框，在【目录路径】文本框中输入账号“wm”的根目录路径“C:/ftp/yuangong/wm”，如图 7-41 所示，单击【选择】按钮。



图 7-53 【目录访问规则】对话框

21 返回至【目录访问规则】对话框，单击【保存】按钮，如图 7-54 所示。



图 7-54　【目录访问规则】对话框

22 返回至【用户属性 – wm】目录访问对话框，单击【保存】按钮，如图 7-55 所示。

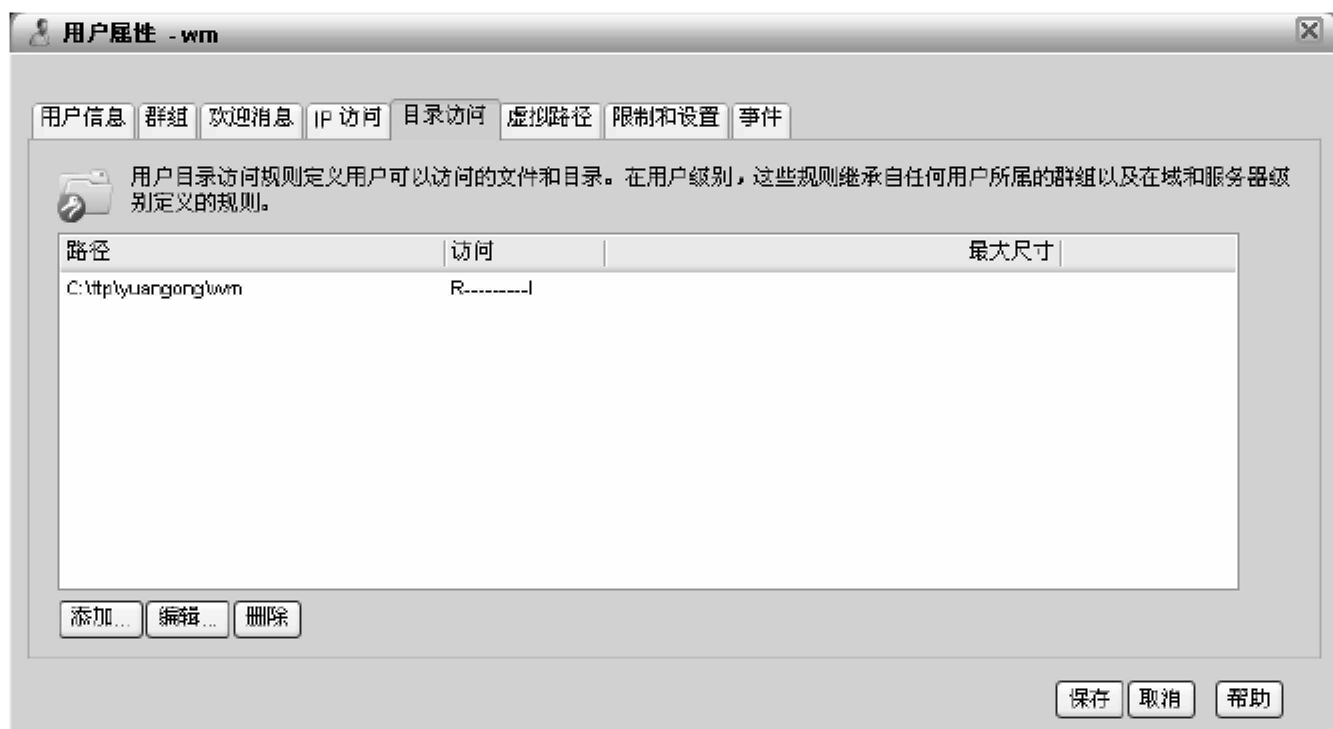


图 7-55　【用户属性 – wm】目录访问对话框

23 如图 7-56 所示，返回至【Serv-U 管理控制台 – 用户】对话框，照此流程依次添加员工苏红和经理王晓亮的账户。



图 7-56　【Serv-U 管理控制台 – 用户】对话框

2．客户端访问

在一台和 IP 地址 172.16.1.200 网络相通的计算机上访问 FTP 服务器，客户端访问 FTP 服务器的具体操作步骤如下。

01 双击桌面上【我的计算机】图标，在地址栏输入“ftp://172.16.1.200”，按下【Enter】键，弹出匿名成功登录 FTP 后的界面，如图 7-57 所示。

02 在空白处单击右键，如图 7-58 所示，在弹出的快捷菜单中选择【登录】命令。



图 7-57 匿名用户登录 FTP



图 7-58 登录 FTP

03 弹出【登录身份】对话框，在【用户名】和【密码】文本框中分别输入要登录的账户和密码，本实例中使用员工王明的账号进行登录，如图 7-59 所示，输入王明的账号和密码后单击【登录】按钮。

04 如图 7-60 所示，员工王明成功登录，并且王明此时对 FTP 的权限和上文中王明登录域“192.168.1.200”后的权限是不一样的。

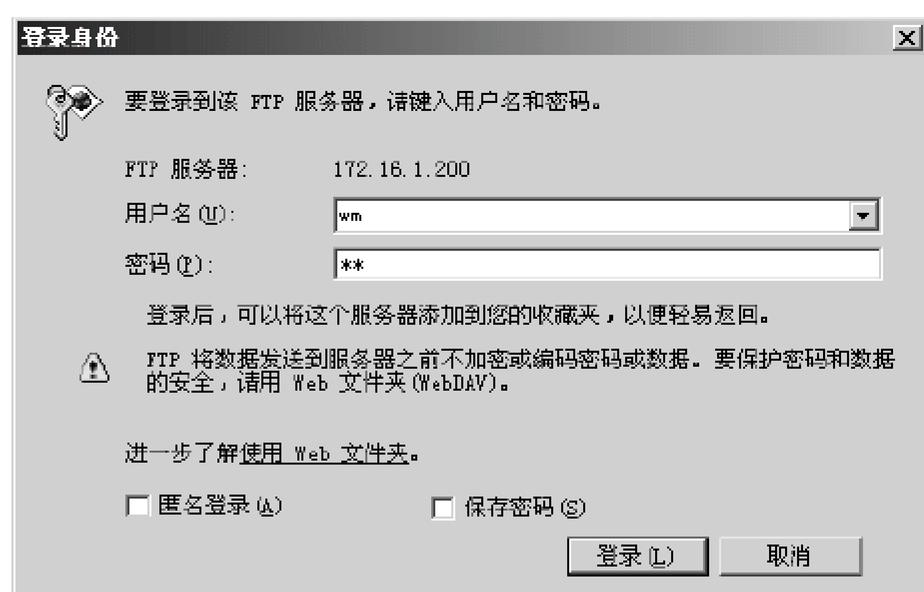


图 7-59 【登录身份】对话框



图 7-60 用户 wm 登录 FTP

3. 管理不同的域

通过建立不同的域，Serv-U 可以实现同一账户在多网段访问具有不同的权限，作为网络管理员到底该如何管理不同的域呢？下面详细讲解如何管理不同的域。

管理不同 Serv-U 域的具体操作步骤如下。

01 双击桌面上 Serv-U 快捷方式图标，打开 Serv-U 的管理控制台操作界面，如图 7-61 所示，单击【管理域】按钮。



图 7-61　Serv-U 管理控制台操作界面

02 弹出【域】对话框，可以看到 Serv-U 软件所有的域，如果要管理域“192.168.1.200”的用户，单击选择【192.168.1.200】，单击【选择】按钮，如图 7-62 所示。



图 7-62　【域】对话框

03 返回 Serv-U 管理控制台，在【管理域】选项后面为 192.168.1.200，表明现在管理的 FTP 域名为“192.168.1.200”，如图 7-63 所示。

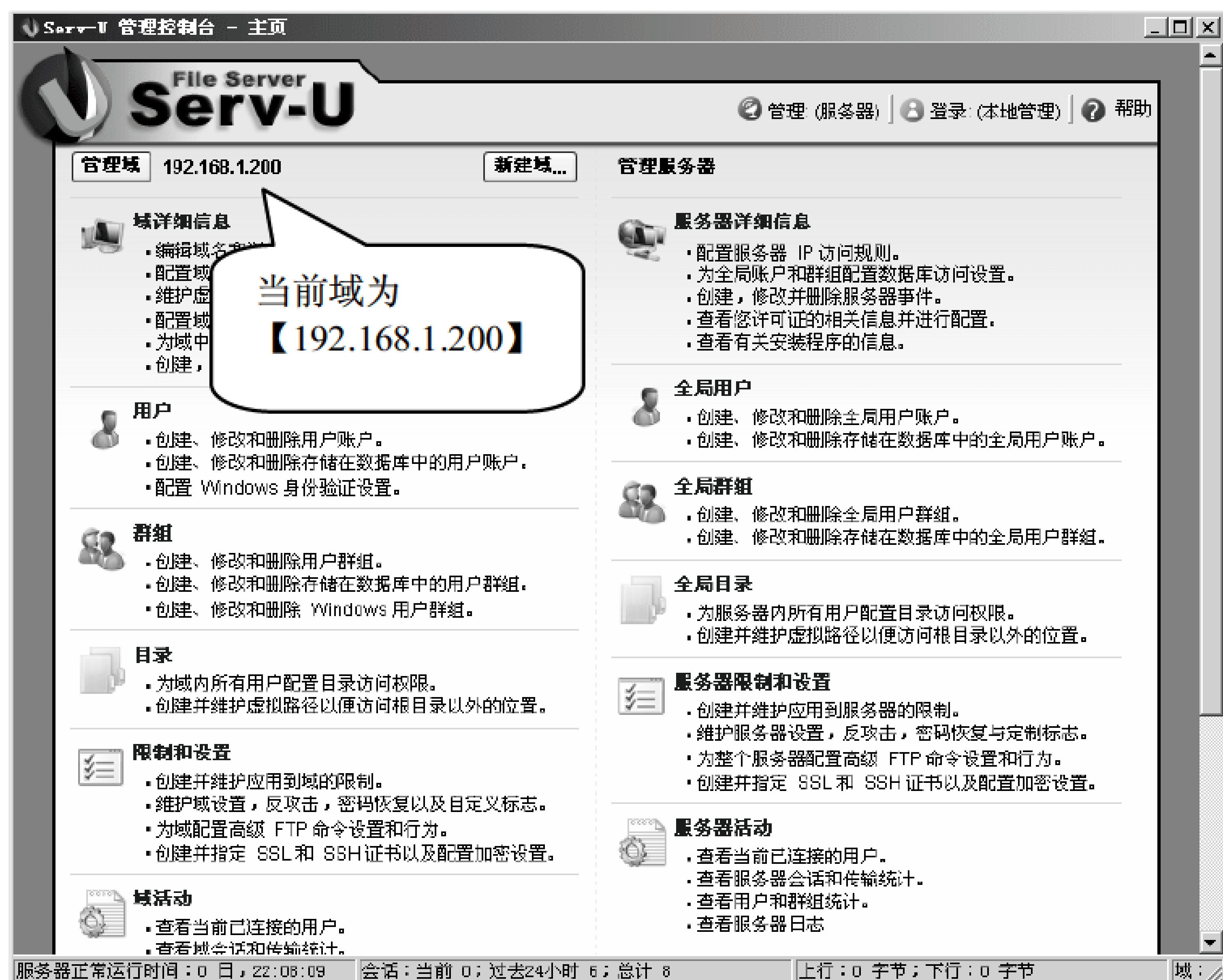


图 7-63　Serv-U 管理控制台操作界面

7.2.4　建立账户虚拟目录，实现多层次的账户目录管理

默认情况下，Serv-U 软件账户登录后访问到的是用户自己的主目录，如果用户要访问到主目录之外的文件或文件夹，就必须要用到虚拟路径。虚拟路径允许用户访问根目录以外的文件和文件夹。所谓虚拟路径，就是将现有目录映射到系统中的其他位置，使用户能够在其可访问的目录结构中看到该目录。为了能够访问该映射的位置，用户还是需要满足对虚拟路径对应的物理路径的目录访问规则。虚拟路径的具体使用方法如下。

1. 单独为一个用户添加虚拟路径

本实例中单独为经理添加虚拟路径，使得经理可以访问部门所有员工的信息。为经理添加虚拟路径的具体操作步骤如下。

01　双击桌面上的 Serv-U 快捷方式图标，打开 Serv-U 的管理控制台操作界面，单击【用户】选项域中的【创建、修改和删除用户账户】链接。

02　弹出【Serv-U 管理控制台 – 用户】窗口，双击要管理的账户名称，本实例中为经理王晓亮添加虚拟路径，双击王晓亮的账户名称“wxl”，如图 7-64 所示。



图 7-64　【Serv-U 管理控制台 – 用户】窗口

03 弹出【用户属性 – wxl】对话框，选择【虚拟路径】选项卡，单击【添加】按钮，如图 7-65 所示。

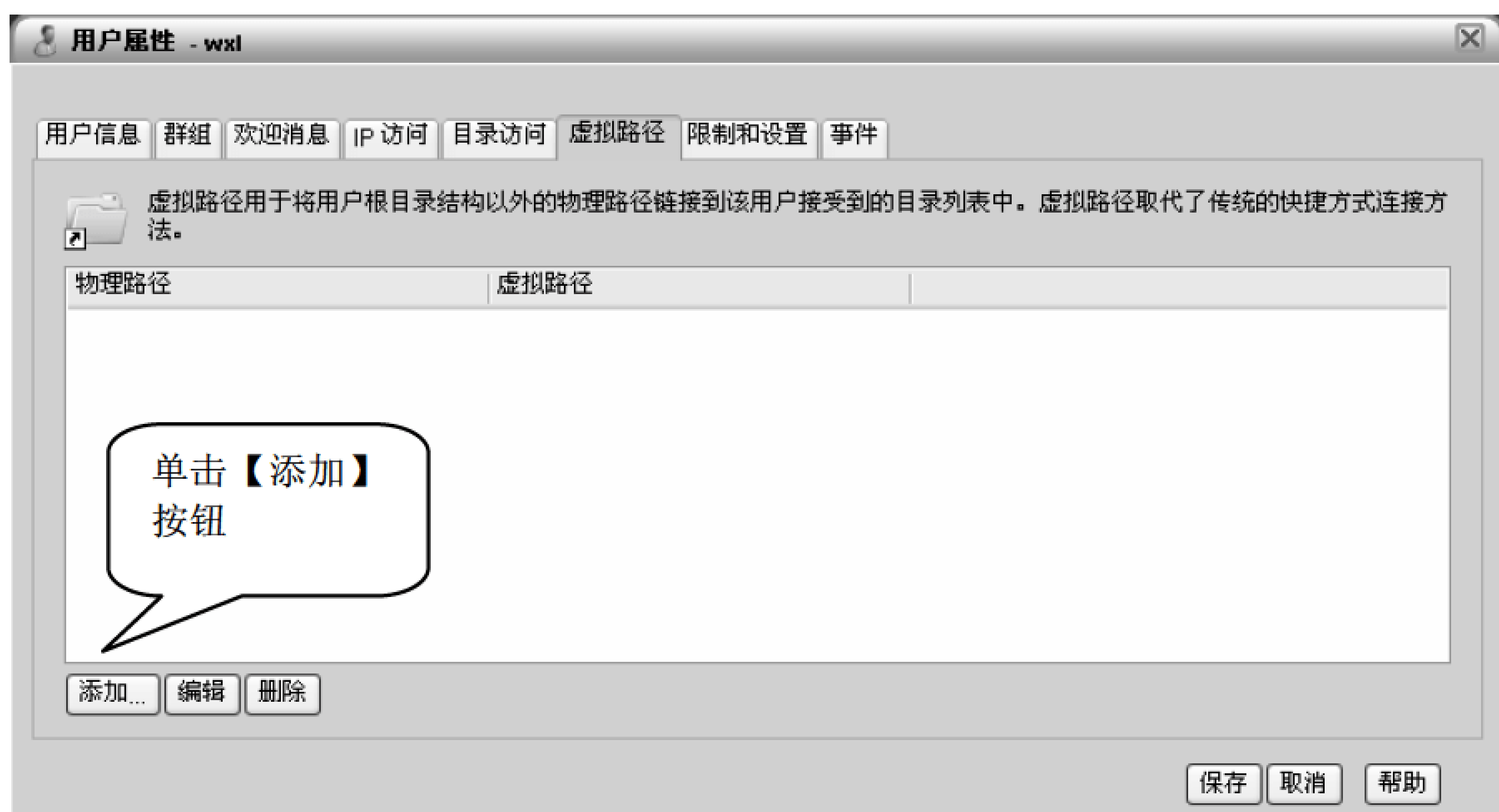


图 7-65　【用户属性 – wxl】虚拟路径对话框

04 弹出【虚拟路径】对话框，单击【物理路径】文本框后面的图标，如图 7-66 所示。

05 弹出【浏览】对话框，在【目录路径】文本框中输入经理要访问的文件夹的真实物理路径，本实例中经理要访问部门员工的目录，所以输入员工目录的路径为“C:/ftp/yuangong”，单击【选择】按钮，如图 7-67 所示。

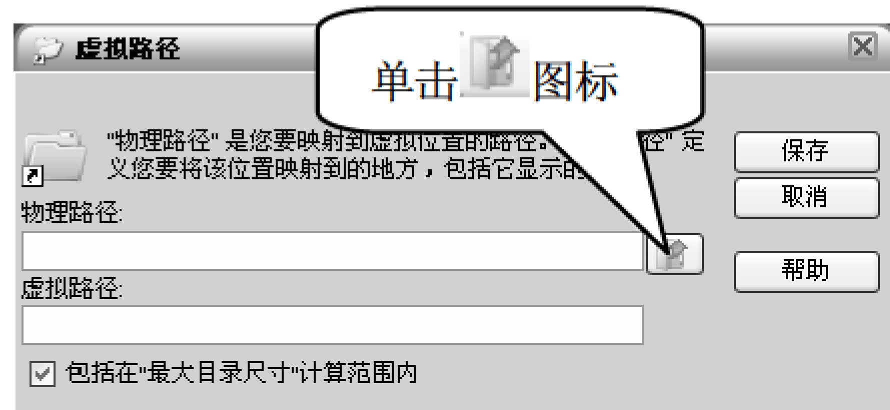


图 7-66 【虚拟路径】对话框



图 7-67 【浏览】对话框

06 返回至【虚拟路径】对话框，在【虚拟路径】文本框中输入要将上面的物理路径映射到的虚拟位置的具体路径。本实例中要将员工目录映射到经理的主目录中，所以在【虚拟路径】文本框中输入“C:/ftp/wxl/员工目录”，其中“C:/ftp/wxl/”为经理的主目录，“员工目录”为员工目录映射经理主目录中的名字，如图 7-68 所示，单击【保存】按钮。

07 返回至【用户属性】对话框，选择【目录访问】选项卡，单击【添加】按钮，如图 7-69 所示。

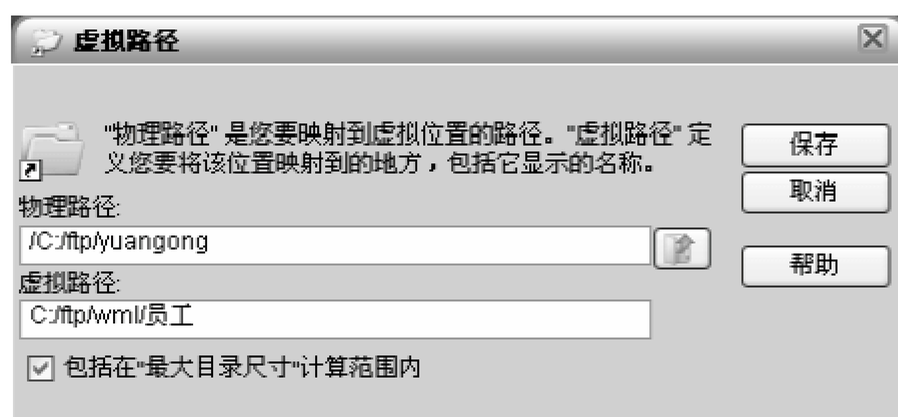


图 7-68 【虚拟路径】对话框

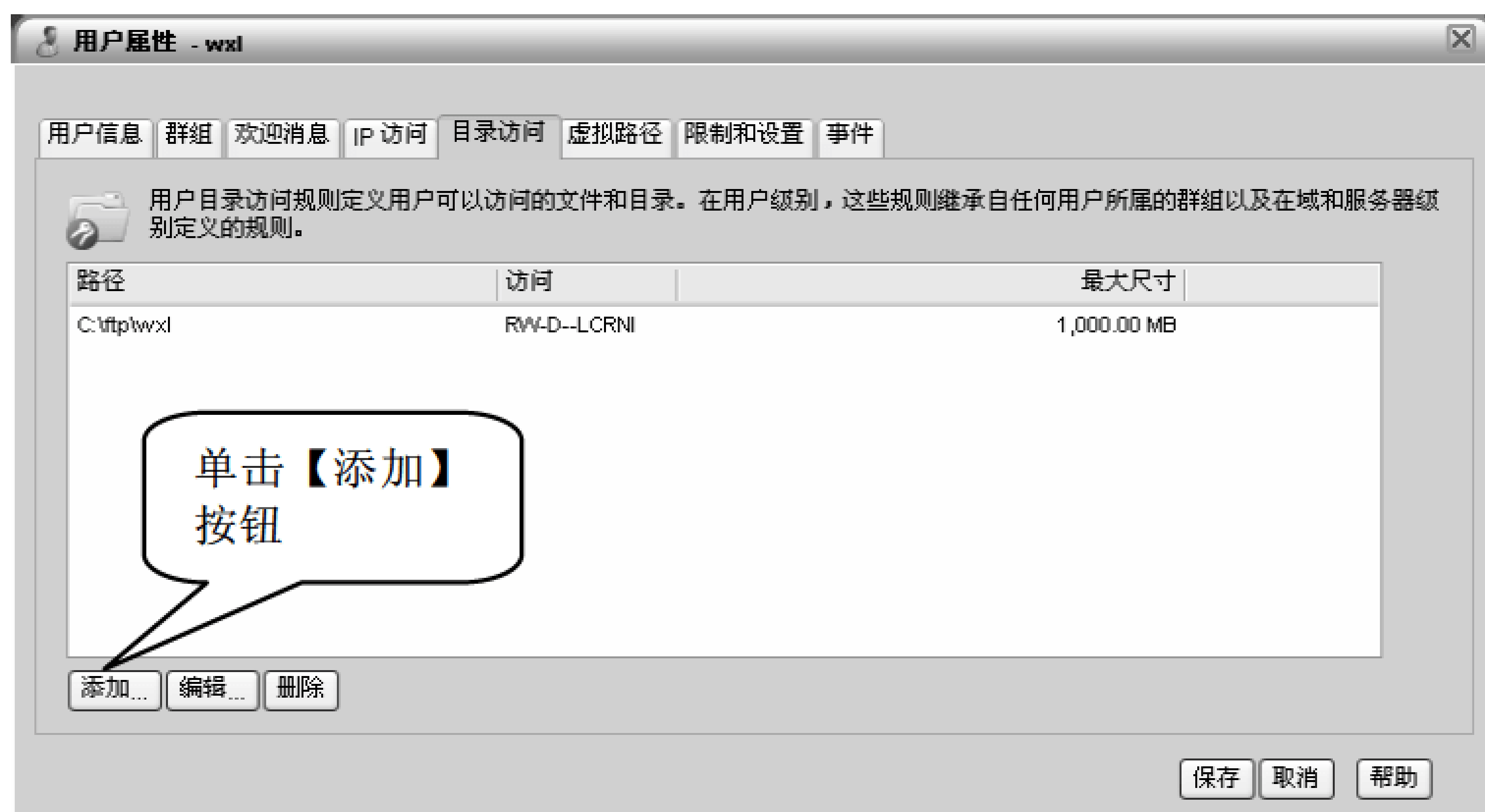


图 7-69 【用户属性 – wxl】虚拟路径对话框

08 弹出【目录访问规则】对话框，选中【文件】选项组中的【读】和【目录】选项组中的【列表】复选框，单击【路径】文本框后面的图标。

09 弹出【浏览】对话框，在【目录路径】文本框中输入经理要访问到的主目录之外的文件夹的物理路径，本实例中经理要访问本部门的员工目录，因此这里输入的物理路径为“C:/ftp/yuangong”，如图 7-70 所示，单击【选择】按钮。

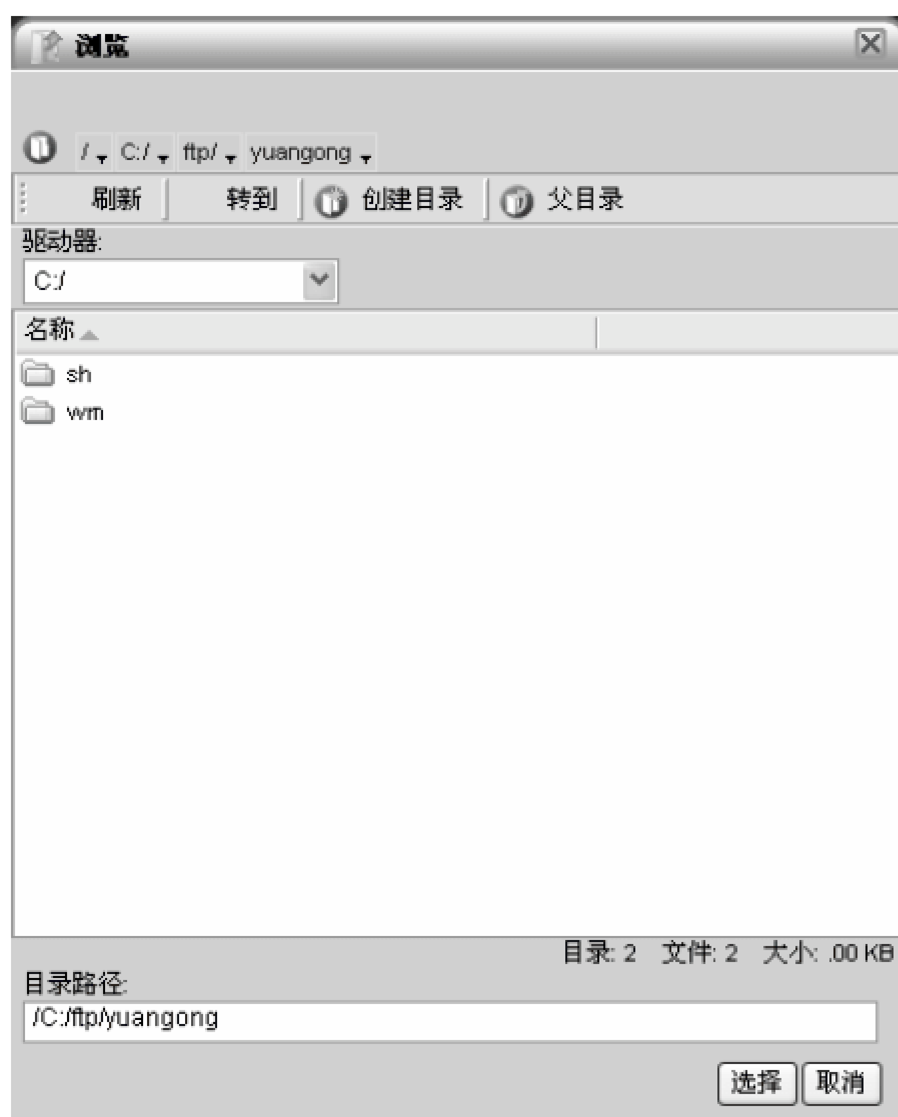


图 7-70 【浏览】对话框

10 返回至【目录访问规则】对话框，如图 7-71 所示，单击【保存】按钮。

11 返回【用户属性 – wml】目录访问对话框，如图 7-72 所示，单击【保存】按钮。





图 7-71 【目录访问规则】对话框　　图 7-72 【用户属性 – wml】目录访问对话框

12 返回至【Serv-U 管理控制台 – 用户】对话框，为王晓亮经理创建虚拟路径完成，如图 7-73 所示。



图 7-73 【Serv-U 管理控制台 – 用户】对话框

2. 为服务器所有用户全局创建虚拟路径

很多时候 Serv-U 服务器上的所有用户在登录后，需要访问同一个目录，这个时候就需要将这个目录一个一个地添加虚拟路径至所有用户的根目录，这是一个很大的工作量。下面详细讲解如何为所有用户根目录全局添加虚拟路径，本实例中将 public 这个目录建立虚拟路径至所有用户的根目录中。

将 public 建立虚拟路径至所有用户的根目录的具体操作步骤如下。

01 双击桌面上 Serv-U 的快捷方式图标，显示【已启用 Windows Internet 增强的安全配置】提示框，选中【不要再显示此提示】对话框，单击【确定】按钮。

02 打开 Serv-U 的管理控制台，选择【目录】选项域中的【创建并维护虚拟路径以便访问根目录以外的位置】选项。

03 弹出【Serv-U 管理控制台 – 目录】操作界面，单击【添加】按钮。

04 弹出【虚拟路径】对话框，单击【物理路径】文本框后面的图标。

05 弹出【浏览】对话框，在【目录路径】文本框中输入“public”目录的物理路径“C:/ftp/public”，如图 7-74 所示，单击【选择】按钮。

06 返回至【虚拟路径】对话框，在【虚拟路径】文本框中输入虚拟路径“%HOME%/公共目录”，其中“%HOME%”表示所有用户的根目录，“公共目录”表示“public”目录映射到用户根目录中显示的名字，如图 7-75 所示，单击【保存】按钮。

07 返回至【Serv-U 管理控制台 – 目录】对话框，选择【目录访问】选项卡，单击【添加】按钮，如图 7-76 所示。



图 7-74　【浏览】对话框

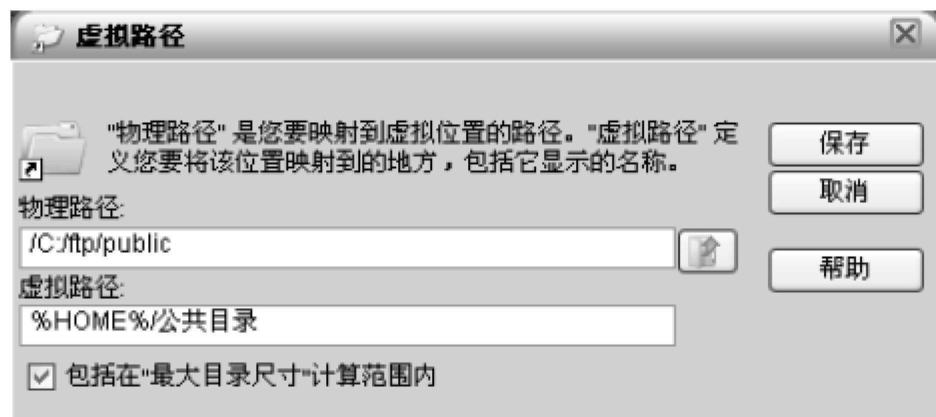


图 7-75　【虚拟路径】对话框



图 7-76　【Serv-U 管理控制台 – 目录】窗口

08 弹出【目录访问规则】对话框，单击【路径】文本框后面的 图标。

09 弹出【浏览】对话框，单击【选择】按钮。

10 返回至【目录访问规则】对话框，如图 7-77 所示，单击【保存】按钮。

11 返回至【Serv-U 管理控制台 – 目录】对话框，如图 7-78 所示，已经将“public”目录添加虚拟路径至所有用户的根目录并命名为“公共目录”。



图 7-77 【目录访问规则】对话框



图 7-78 【Serv-U 管理控制台 – 目录】窗口

3. 客户端访问

在一台和 192.168.1.200 地址网络相通的计算机上进行 FTP 访问，客户端访问 FTP 的具体操作步骤如下。

01 双击桌面上【我的计算机】图标，在地址栏里面输入“ftp://192.168.1.200”，其中“192.168.1.200”为 FTP 服务器的 IP 地址。按下【Enter】键，弹出匿名用户成功登录 FTP 服务器的界面，可以看到里面有一个叫“公共目录“的文件夹就是上面通过虚拟路径映射的文件夹，如图 7-79 所示。

02 在空白处右击鼠标，在弹出的快捷菜单中选择【登录】命令，如图 7-80 所示。



图 7-79 登录 FTP 成功



图 7-80 登录对话框

03 弹出【登录身份】对话框，在【用户名】和【密码】对话框中分别输入合法的账号和密码，本实例中输入经理的账号“wxl”，如图 7-81 所示，单击【登录】按钮。

04 如图 7-82 所示，为经理成功登录 FTP 的界面，从图 7-82 中可以看到里面有一个叫“公共目录”的文件夹就是上面通过虚拟路径映射的文件夹。

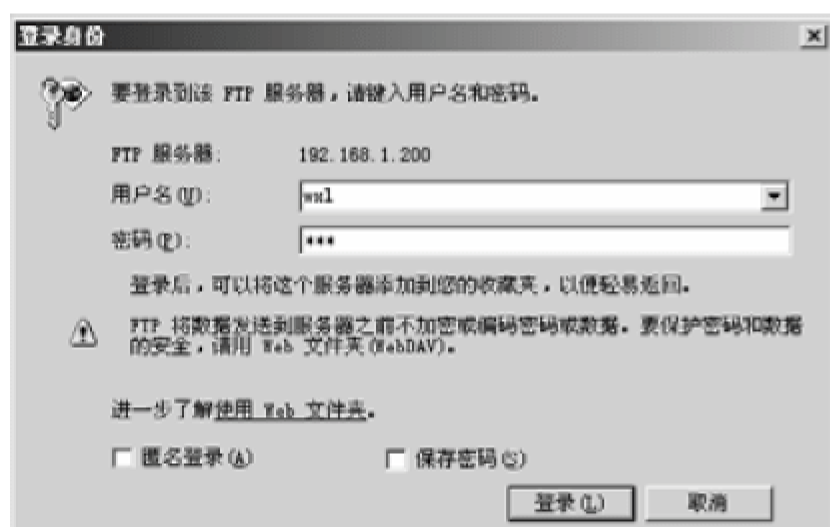


图 7-81　【登录身份】对话框



图 7-82　账号 wxl 成功登录 FTP

7.3　专家答疑

（1）Serv-U 安装完成后，根据前面介绍的步骤进行域的建立，但是 Serv-U 软件总是启动不成功，怎么办？

答：在创建域的过程中，如图 7-15 所示，启用了【FTP 和 Explicit SSL/TLS】功能，FTP 协议需要使用系统的 21 端口，如果觉得配置正确但是 Serv-U 服务器启动总不成功，可以考虑是否是计算机的 21 端口被其他程序占用。

（2）因为 Serv-U 所有用户都需要访问一个目录，为此采用了全局为所有用户根目录添加虚拟路径，但是不想让匿名用户 anonymous 访问这个虚拟路径怎么办？

答：为了使得所有用户都能访问到虚拟路径，在添加虚拟路径的时候使用了%HOME%参数，这个参数的含义是为服务器所有用户添加虚拟路径，当然也包含匿名用户 anonymous。如果不需要匿名用户访问，可以在为匿名用户单独添加一个目录访问权限，使得匿名用户没有权限访问该虚拟路径的物理位置即可。

第 8 章　企业邮件服务器的搭建与维护

企业邮件服务是目前各大企业使用相对广泛的一种服务类型，可以提高企业形象，方便企业内部员工以及与客户的沟通。同时，使用 ISP 提供的电子邮箱在安全性和可管理性上都比不上企业邮箱。所以当企业发展到一定规模时，必须要考虑构建企业邮箱。下面详细介绍搭建企业邮件服务器及其基本维护工作的操作方法。

8.1　企业邮件服务器概述

企业邮件服务器与通常认识的运营商提供的邮件服务不相同，所以在操作之前首先要正确认识企业邮箱，并完成搭建企业邮件服务器的准备工作。

8.1.1　企业邮件服务器介绍

可以通过以下问题来了解企业邮件服务器。

1. 什么是企业邮箱

搭建企业邮件服务器的目的是让企业拥有独立使用的企业邮箱。企业邮箱可以使用企业自己的域名后缀做邮箱地址，例如 user@企业域名。企业邮箱一般只允许内部员工、客户及合作伙伴使用，可以根据需要为用户分配不同的权限，并且可以实现对所有邮件统一监管。

2. 哪些企业需要架设企业邮件服务器

企业邮箱是企业内部、分支机构之间，以及与客户沟通的重要工具，在企业日常经营管理，以及对外商务活动中发挥着至关重要的作用，所以大多数的企业都应该拥有企业邮箱，即搭建企业邮件服务器。特别是对外经济活动频繁的企业或组织更需要企业邮箱。

8.1.2　搭建邮件服务器前的准备工作

在搭建邮件服务器之前，还需要先解决以下问题。

1. 确定邮件服务器的使用范围

在搭建邮件服务器之前首先要确定邮件服务器的使用范围，考虑邮件服务器是只允许在企业内网使用，还是可以通过互联网访问。

（1）如电力企业、银行或政府部门，在一定的地理范围内覆盖有广泛的内部网络，为了通信安全一般会建立只允许内部员工、子公司或合作伙伴使用的邮件服务器。移动及家庭办公用户、子公司及合作企业通过 VPN 技术连接到整个企业网络中，企业网络配置内网独立使用的 DNS 服务器进行邮件域名解析，如图 8-1 所示的网络拓扑图。

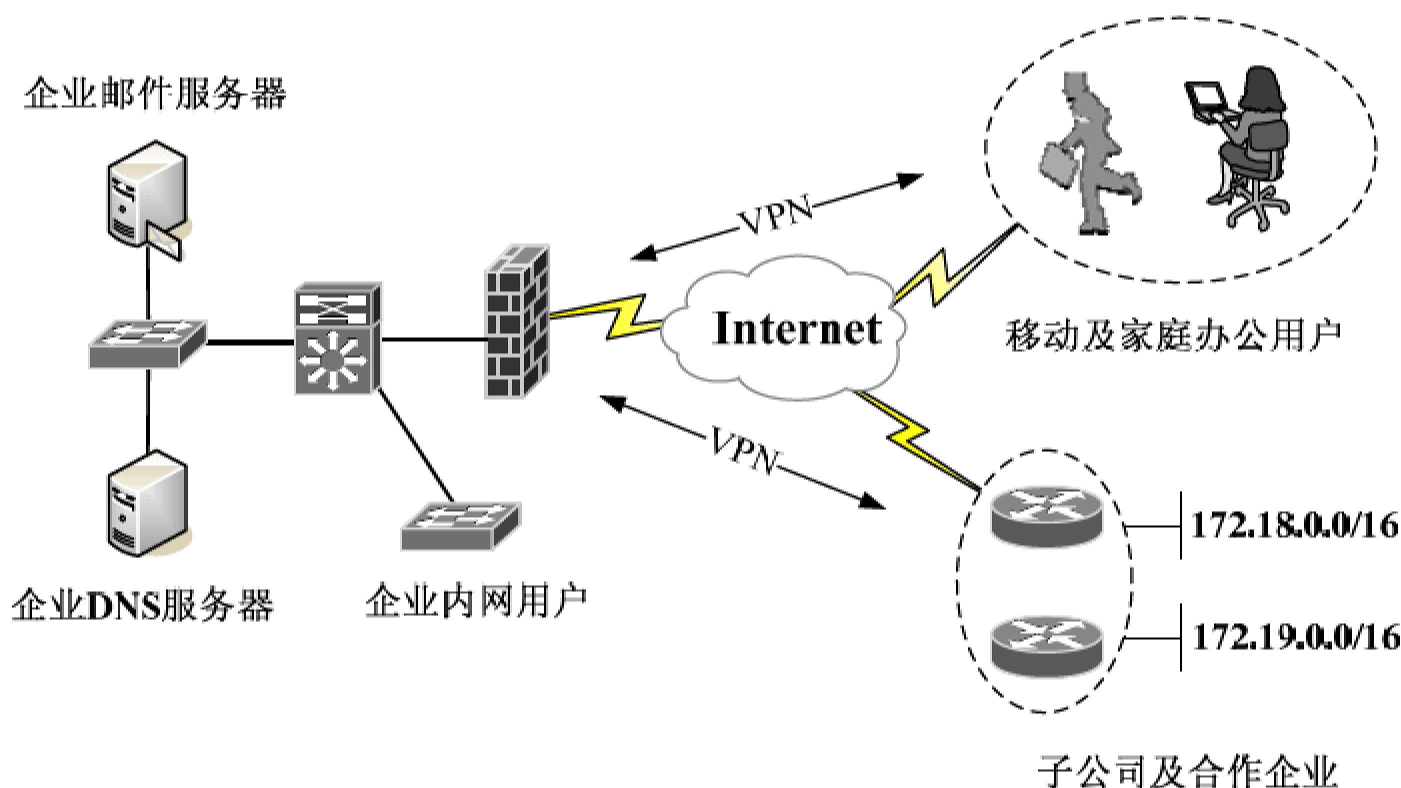


图 8-1　企业内部使用邮件服务器的网络拓扑图

（2）而对于一般企业来说，邮件服务器允许员工在公司使用企业邮箱，同时也需要使用企业邮箱和客户交流，这就要求企业邮箱能够在公共互联网被访问。这类邮件服务器在使用时，要在互联网为其申请邮箱域名，使用互联网公共 DNS 服务器进行邮箱域名解析，如图 8-2 所示的网络拓扑图。

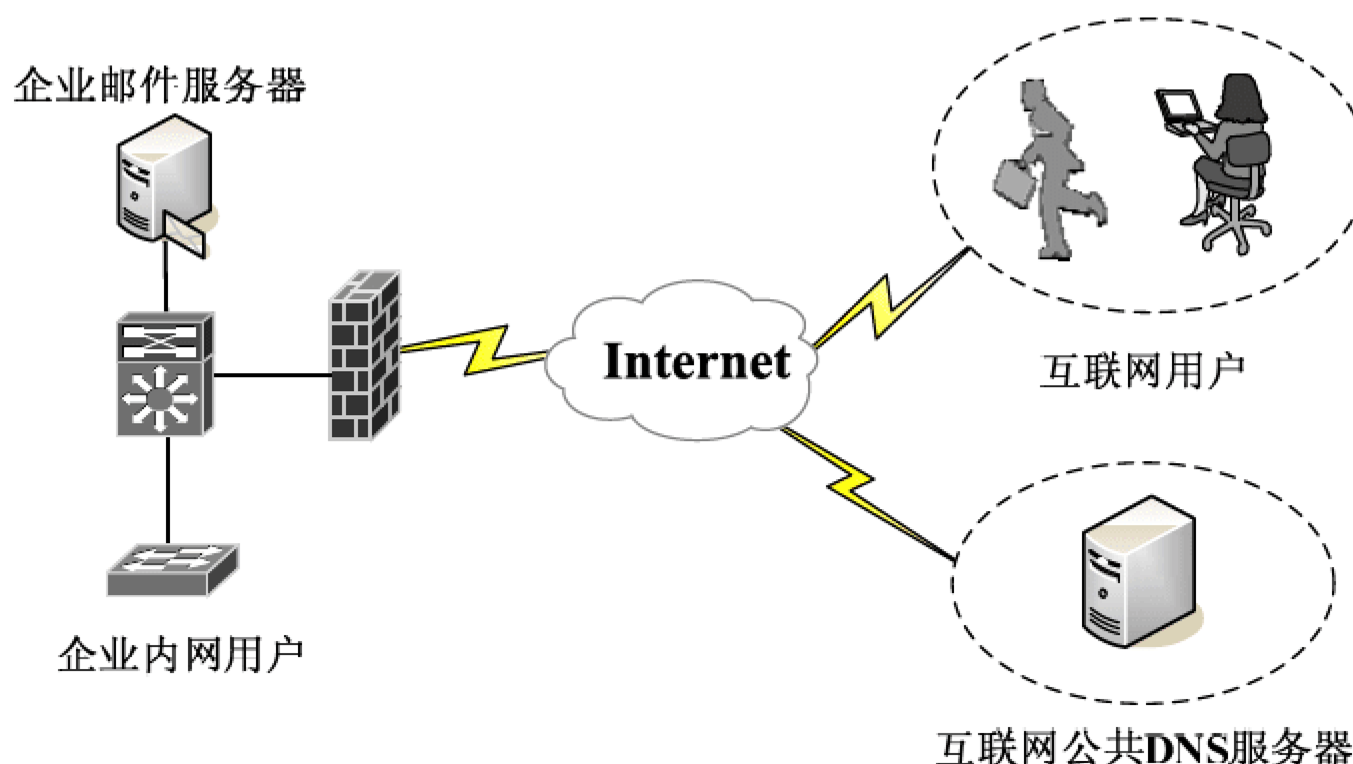


图 8-2　企业互联网公开使用邮件服务器的网络拓扑图

2. 选择邮件服务器程序

市场上流行的邮件服务器很多，常见的有以下几种。

（1）Windows Server 自带邮件服务器：Windows 服务器系统自带的邮件服务器功能简陋，对用户的管理限制功能比较单一，能够使用的客户端主要是 Outlook，不能够满足用户多元化的要求，所以一般不使用 Windows 自带的邮件系统。

（2）Microsoft Exchange Server ：这是由微软公司自行研发的一款邮件服务器，功能强大，适合大型企业使用。但是该服务器的配置相对比较复杂，需要在域环境下配置使用。中小企业不建

议使用该服务器。

（3）Linux Sendmail：基于 UNIX/Linux 系统环境的邮件服务程序，属于开源软件。具有较高的安全性和稳定性。但是使用 Sendmail 程序需要熟悉 Linux 系统，全命令操作，无图形界面，对管理员的技术水平有一定的要求。

（4）Winmail 邮件服务器：是一款适用于中小型用户的邮件系统。它提供多语言的全功能的 Web mail，集成有美观的 Web 访问界面，可以通过网页进行在线注册新邮箱、收发邮件、修改密码、设置外部 POP3 邮箱、自动转发、自动回复等操作，主要通过 IIS 进行发布使用，操作较简单。

（5）U-Mail 邮件服务器：是一款安全易用全功能的邮件服务器软件，内嵌卡巴斯基杀毒引擎，基于行为识别的反垃圾过滤引擎，纯 Web 端的便捷管理，全自动化的自我管理。客户的电子邮件通信服务要求稳定高效，可集中管理 U-Mail 邮件服务器，能高效地为从小企业到大中型企业提供全面的服务。与其他邮件服务器软件相比，U-Mail 能更好地节省时间、精力和金钱，并能减少失误。

3. 配置邮件服务器软硬件环境

硬件环境：CPU 为 Pentium，硬盘 3G，内存 256M。

操作系统平台：U-Mail for Windows 可以安装在 Windows 2000、 Windows 2003、Windows 2008 操作系统上，本书主要介绍在 Windows Server 2008 操作系统中 U-Mail 邮件服务器的操作。

8.2 项目实战：搭建 U-Mail 邮件服务器

U-Mail 这种邮件服务器对于中小企业来说是很实用的，本节将介绍 U-Mail 邮件服务器的搭建以及应用配置。

8.2.1 邮件服务器方案介绍

首先来介绍一个简单的邮件服务器方案，包括需求分析、网络拓扑设计、配置方法等内容。

1. 需求分析

某企业为了方便员工公文发送和工作交流，在企业内部建立了邮件服务器。在内网搭建邮件系统，内网 IP 是 192.168.1.85。

安装 DNS 域名解析服务器和 IIS 服务器后，安装邮件服务器。

配置邮件服务器，邮件服务器安装后利用各种管理员的身份登录邮件服务器配置邮件服务器，可对企业员工分配邮箱用户，创建多个邮箱用户，还可对用户可以进行基本信息设定。

企业内部员工拥有邮箱账户，能够对邮箱进行设置，反垃圾邮件，并且根据需要对个人邮箱进行限制。

2. 网络拓扑设计

可以依照图 8-3 所示的网络拓扑图进行设备连接和配置。

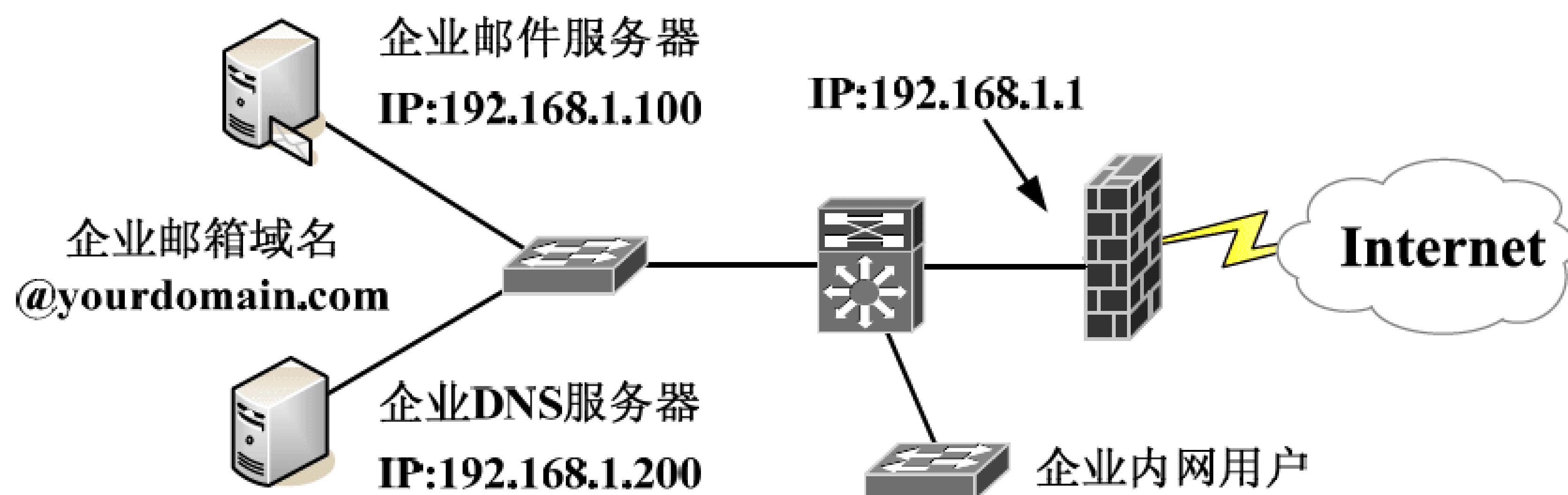


图 8-3　搭建 U-Mail 邮件服务器的网络拓扑图

3. 配置步骤

邮件服务器的搭建需要按照一定的步骤来完成，介绍如下。

（1）需要在企业配置一台 DNS 服务器，并配置邮箱域名解析记录。

（2）在邮件服务器上安装 U-Mail 程序。

（3）使用多种管理员身份对 U-Mail 邮件服务进行配置，确保邮件服务器能够被客户访问。

（4）为企业员工分配邮件账户和使用权限。

（5）设置反垃圾邮件等安全配置，并为个人邮箱定制访问环境界面。

该配置步骤并非只适用于 U-Mail 邮件服务器，大多数邮件服务器的配置都与其相似。

8.2.2　安装配置 DNS 服务器

首先要在企业 DNS 服务器上安装配置 DNS 服务器，本实验使用 Windows Server 2008 服务器，具体操作方法如下。

1. 安装 DNS 服务器

在 Windows Server 2008 中安装 DNS 服务器的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，选择左侧【角色】选项，在右侧选择【添加角色】选项，如图 8-4 所示。



图 8-4　【服务器管理器】窗口

02 弹出【添加角色向导】对话框，如图 8-5 所示，单击【下一步】按钮。

03 弹出【选择服务器角色】对话框，如图 8-6 所示，选中【DNS 服务器】复选框，单击【下

一步】按钮。



图 8-5 【开始之前】对话框

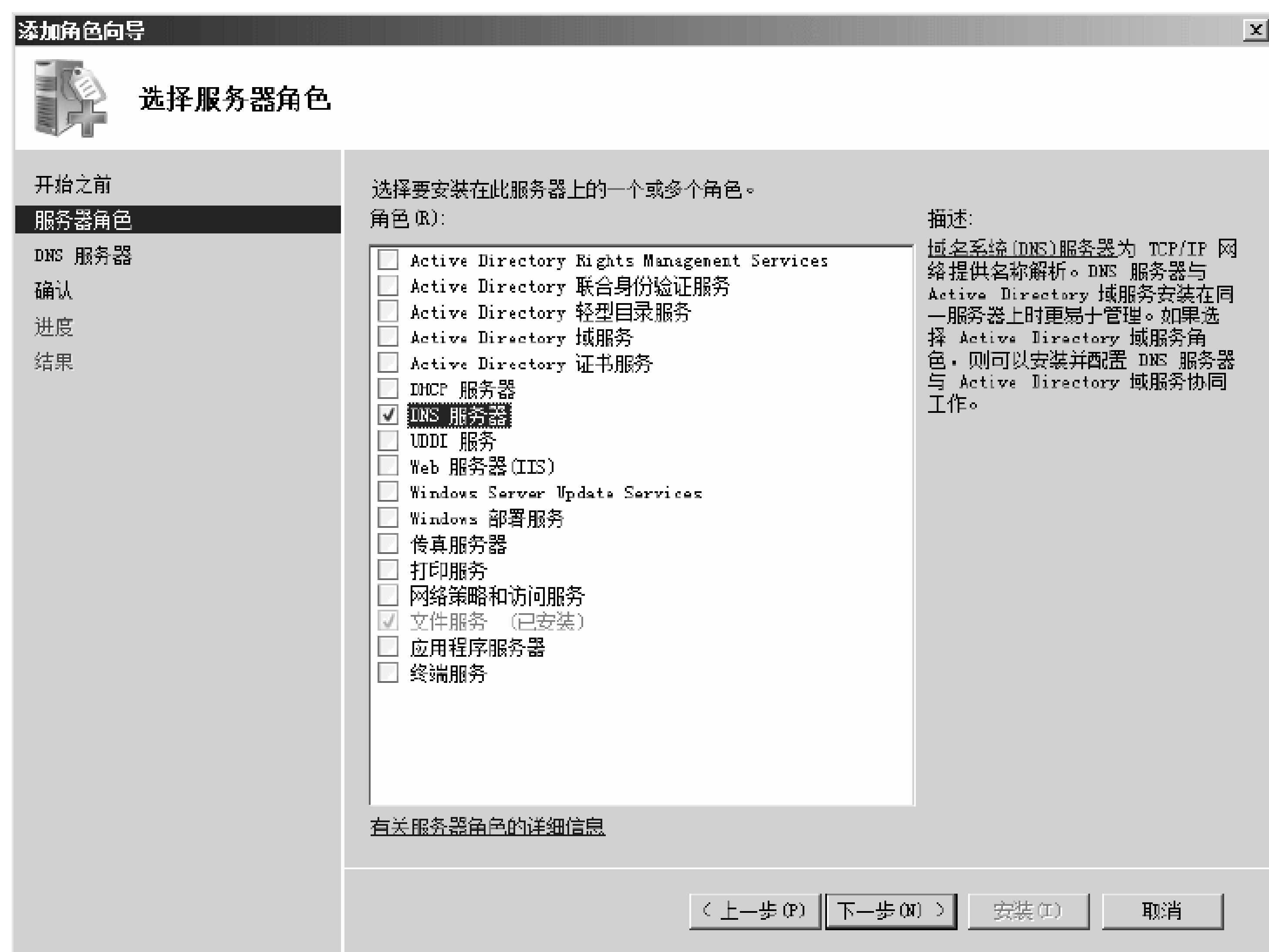


图 8-6 【选择服务器角色】对话框

04 弹出【DNS 服务器】对话框，显示了 DNS 服务器的介绍，单击【下一步】按钮，如图 8-7 所示。

05 弹出【确认安装选择】对话框，单击【安装】按钮，如图 8-8 所示。



图 8-7 【DNS 服务器】对话框



图 8-8 【确认安装选择】对话框

06 弹出【安装进度】对话框，如图 8-9 所示。

07 弹出【安装结果】对话框，安装完成，单击【关闭】按钮，如图 8-10 所示。



图 8-9　【安装进度】对话框



图 8-10　【安装结果】对话框

2. 配置 DNS 服务器

安装好 DNS 之后，要对其进行基本的配置，具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【DNS】选项，如图 8-11 所示。

02 打开【DNS 管理器】窗口，在左侧选项列表中右击【正向查找区域】，在弹出的快捷菜单中选择【新建区域】命令，如图 8-12 所示。



图 8-11　开始菜单选项



图 8-12　【DNS 管理器】窗口

03 弹出【新建区域向导】对话框，单击【下一步】按钮，如图 8-13 所示。

04 弹出【区域类型】对话框，选中【主要区域】复选框，单击【下一步】按钮，如图 8-14 所示。

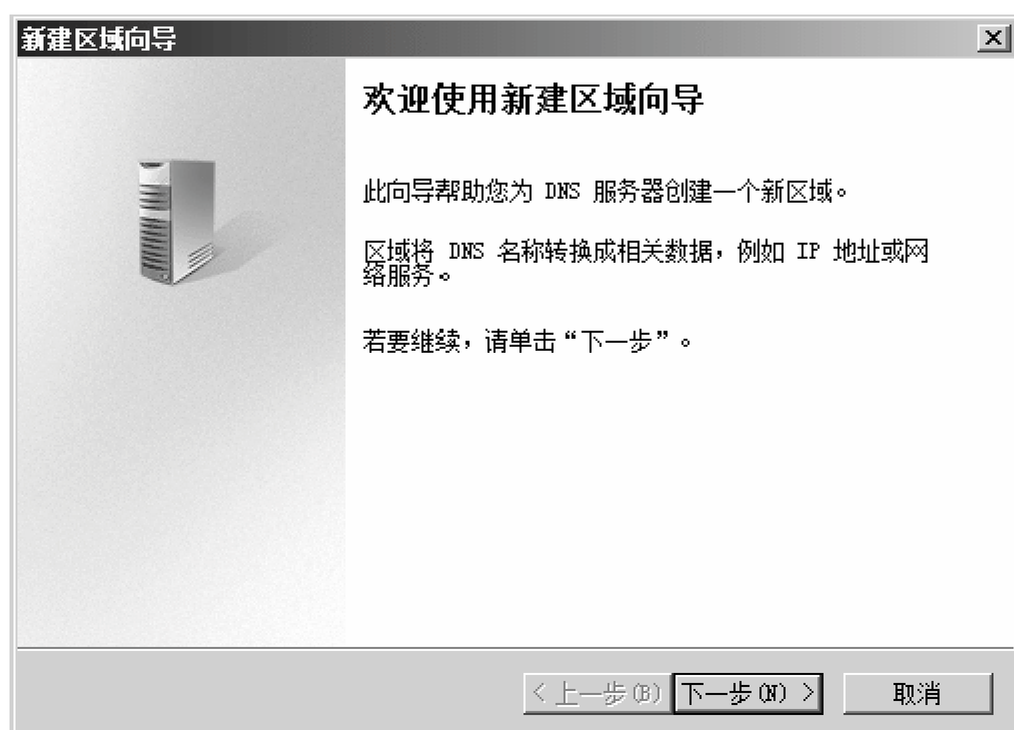


图 8-13　【新建区域向导】对话框

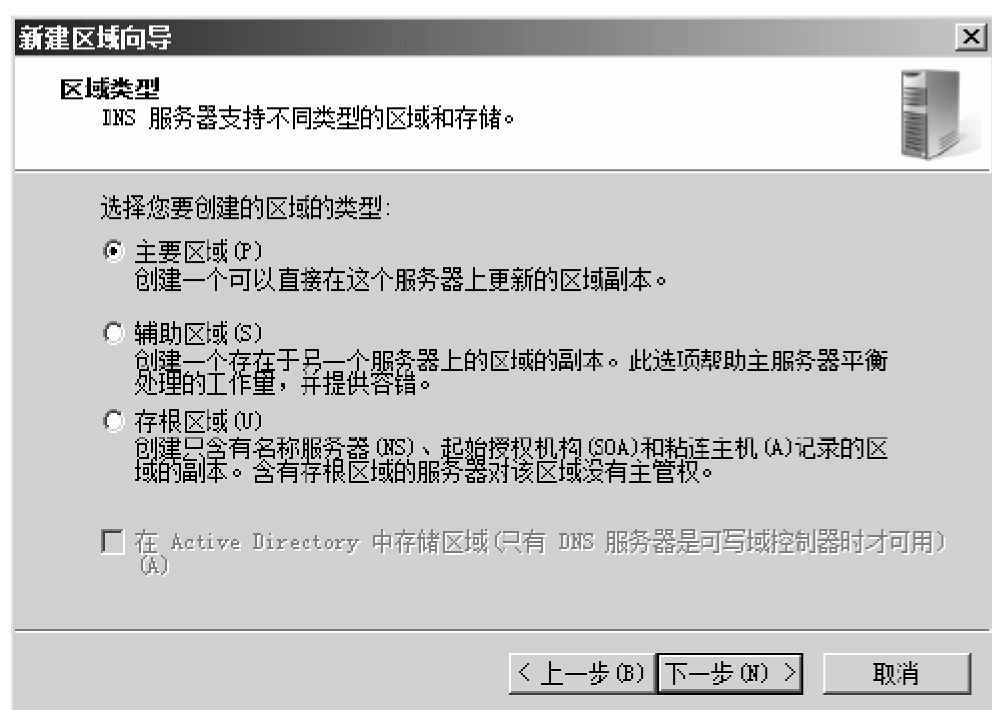


图 8-14　【区域类型】对话框

05 弹出【区域名称】对话框，在【区域名称】文本框中输入企业使用的邮箱域名后缀“yourdomain.com”，如图 8-15 所示。

06 弹出【区域文件】对话框，自动显示新文件名，采用默认配置，单击【下一步】按钮，如图 8-16 所示。

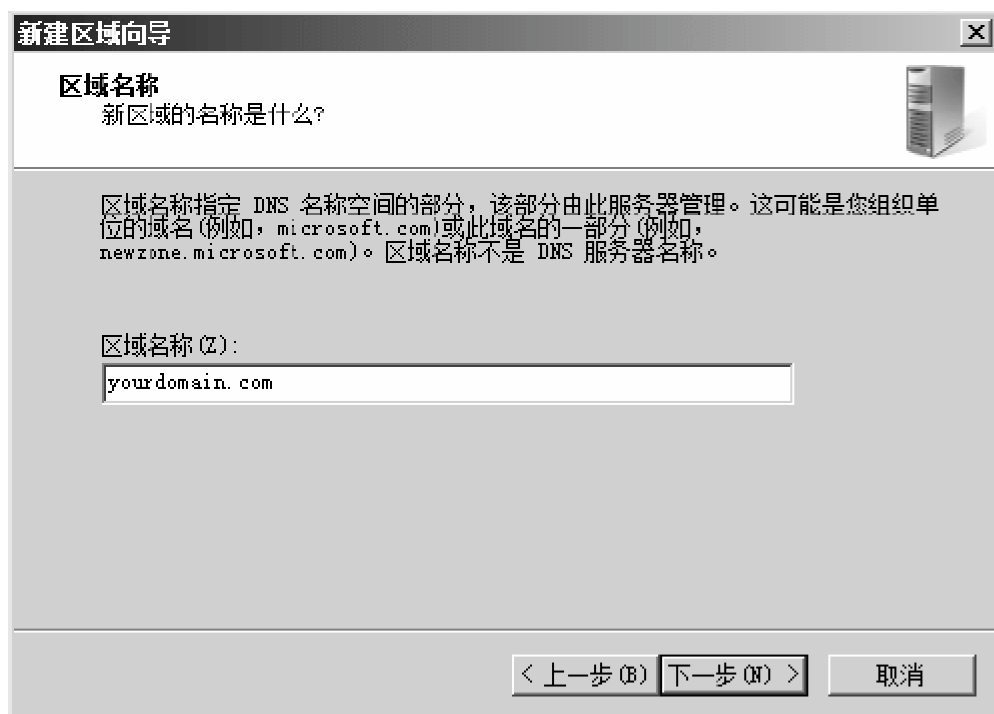


图 8-15　【区域名称】对话框

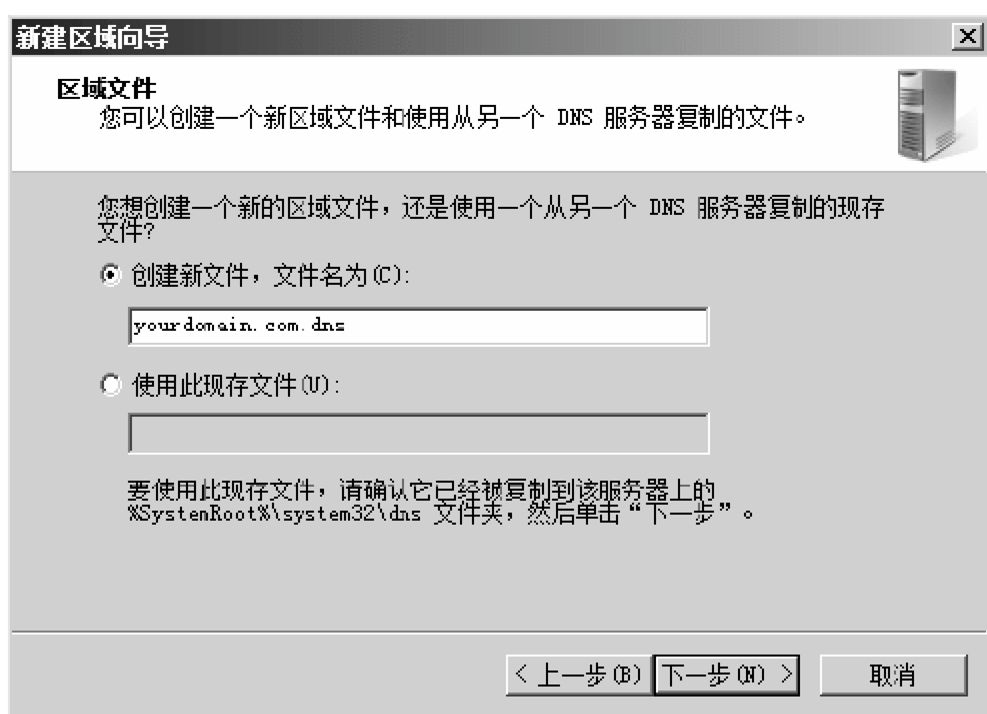


图 8-16　【区域文件】对话框

07 弹出【动态更新】对话框，询问是否允许区域动态更新，如果 DNS 区域在企业内网使用，建议允许动态更新；在 Active Directory 的环境下才可以使用活动目录集成区域和动态安全更新；如果用于 Internet，那么一般不需要动态更新，在此选中【不允许动态更新】复选框，单击【下一步】按钮，如图 8-17 所示。

08 弹出向导完成对话框，新区域已经创建成功，单击【完成】按钮，如图 8-18 所示。

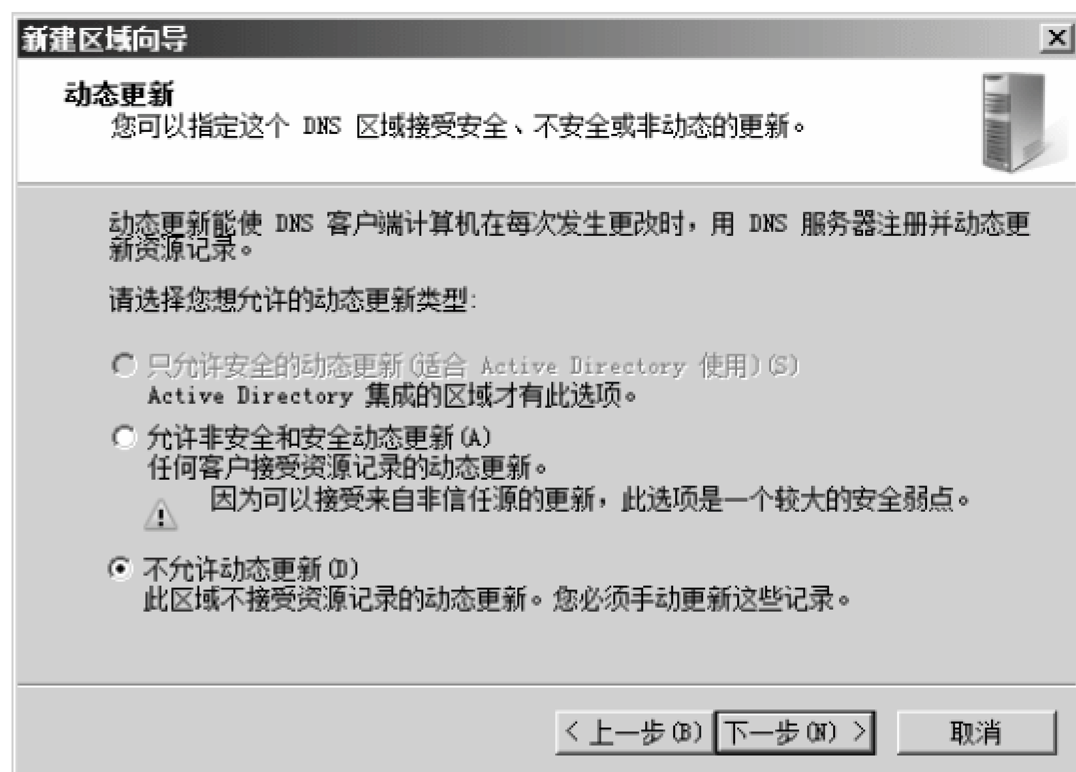


图 8-17 【动态更新】对话框

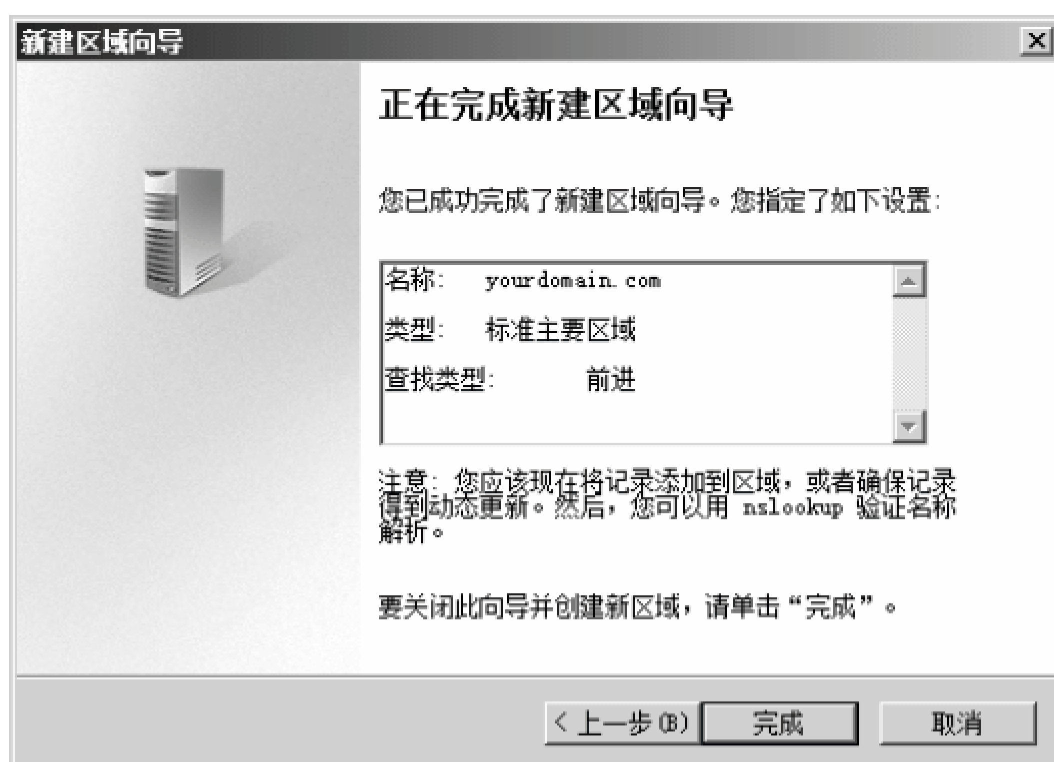


图 8-18 新建区域向导完成对话框

09 返回【DNS 管理器】窗口，要在区域中创建适当的 DNS 记录，首先创建 A 记录，右击【yourdomain.com】域名，在弹出的快捷菜单中选择【新建主机】命令，如图 8-19 所示。

10 弹出【新建主机】对话框，在【名称】文本框中输入"mail"，在【IP 地址】文本框中输入 IP 地址"192.168.1.100"，说明当前邮件服务器 192.168.1.100 的域名为"mail.yourdomain.com"，单击【添加主机】按钮，如图 8-20 所示。



图 8-19 【DNS 管理器】窗口

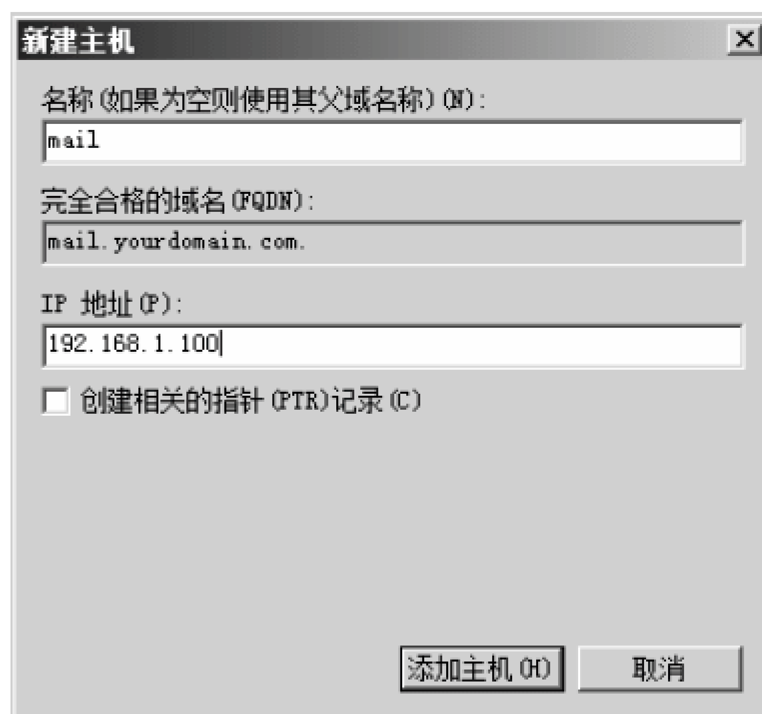


图 8-20 【新建主机】对话框

11 弹出【DNS】提示框，提示添加主机记录成功，单击【确定】按钮，如图 8-21 所示。

12 返回【DNS 管理器】窗口，右击【yourdomain.com】域名，在弹出的快捷菜单中选择【新建邮件交换器（MX）】命令，如图 8-22 所示。

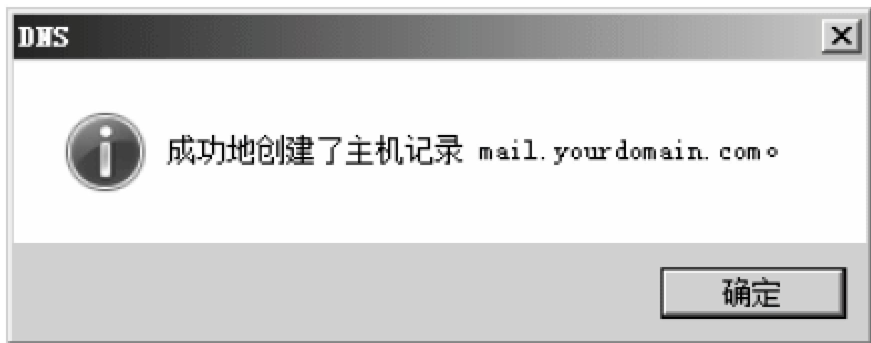


图 8-21　【DNS】提示框

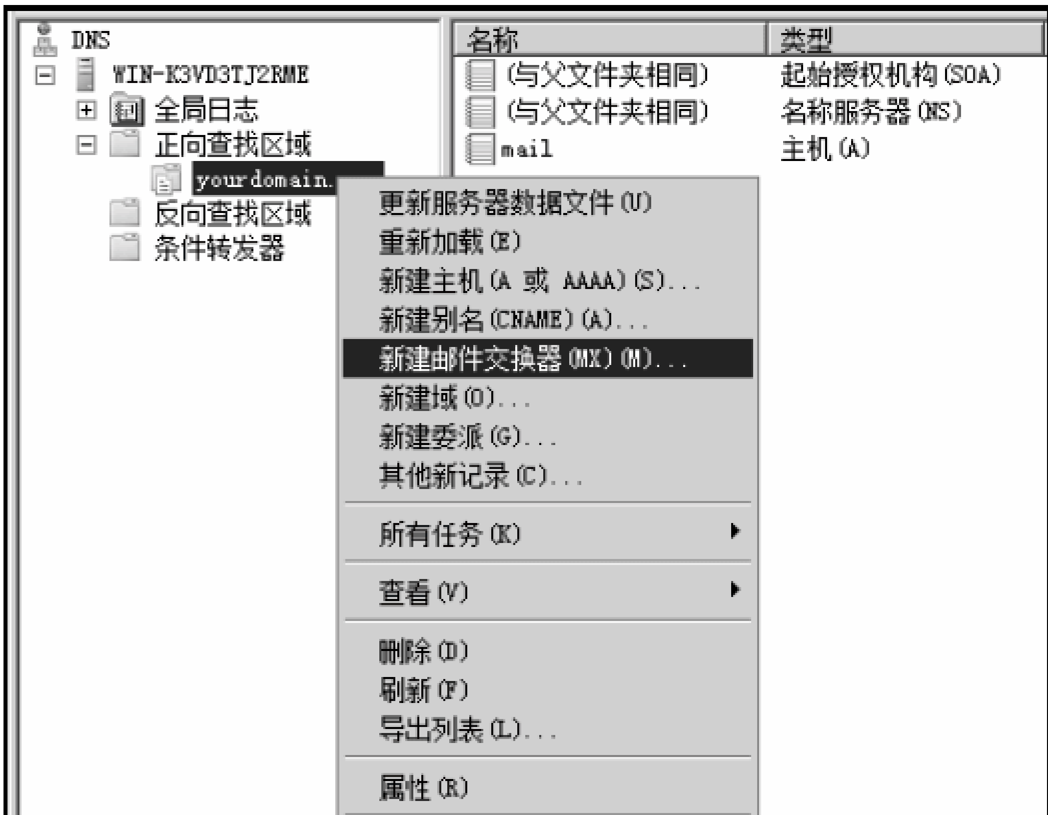


图 8-22　新建邮件交换记录

13 弹出【新建资源记录】对话框，在【邮件服务器的完全合格的域名】文本框中输入上文为邮件服务器配置的完整域名“mail.yourdomain.com”，也可以单击【浏览】按钮找到该域名，单击【确定】按钮，如图 8-23 所示。

14 返回【DNS 管理器】窗口，【yourdomain.com】区域右侧显示了新添加的邮件交换记录信息，如图 8-24 所示。

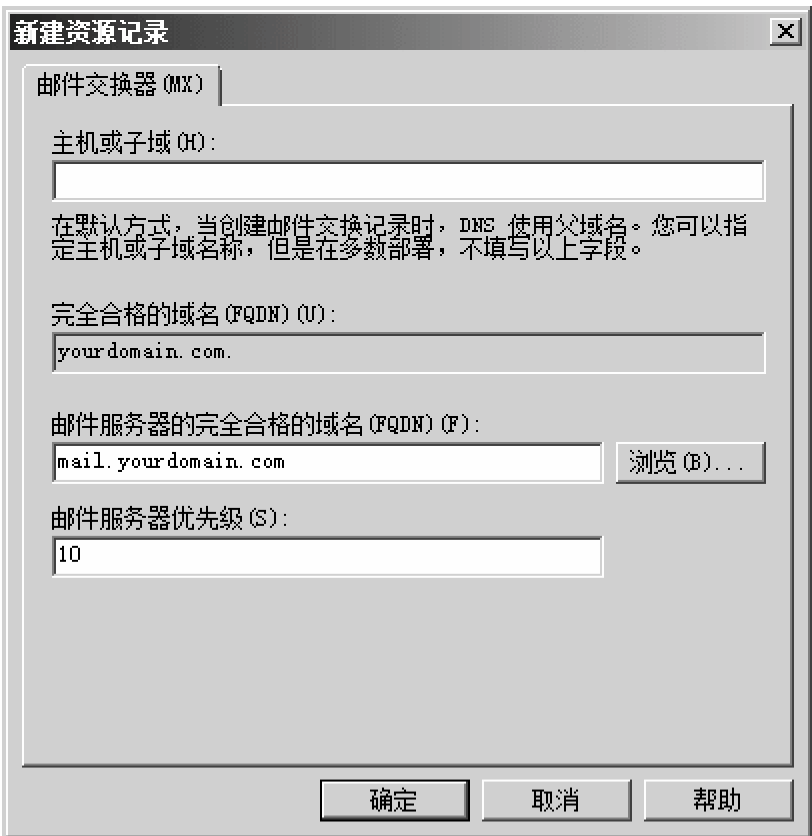


图 8-23　【新建资源记录】对话框



图 8-24　【DNS 管理器】窗口

15 登录 DNS 客户端，打开命令行界面，用“nslookup”命令进行域名解析测试，测试命令如下。

```
C:\Users\Administrator>nslookup          //启用 nslookup 工具
默认服务器:  UnKnown
Address:    192.168.1.200
> mail.yourdomain.com                     //测试邮件服务器域名
服务器:  UnKnown
Address:    192.168.1.200
名称:       mail.yourdomain.com
Address:    192.168.1.100
> set type=mx                            //切换默认测试类型为 MX（邮件交换记录）
> yourdomain.com                         //测试邮箱域名后缀
```

```
服务器:   UnKnown
Address:   192.168.1.200
yourdomain.com    MX preference = 10, mail exchanger = mail.yourdomain.com
mail.yourdomain.com        internet address = 192.168.1.100
>
```

8.2.3 安装 U-Mail 邮件服务器

在 Windows Server 服务器上安装 U-Mail 邮件服务器，具体操作步骤如下。

01 双击运行 U-Mail 邮件服务器安装程序。由于邮件服务器需要 Web 访问，如果服务器中未安装 IIS 组件，自动弹出如图 8-25 所示的对话框，安装 IIS。

02 IIS 组件安装完成后，弹出 U-Mail Mail Server 安装向导，单击【下一步】按钮，如图 8-26 所示。

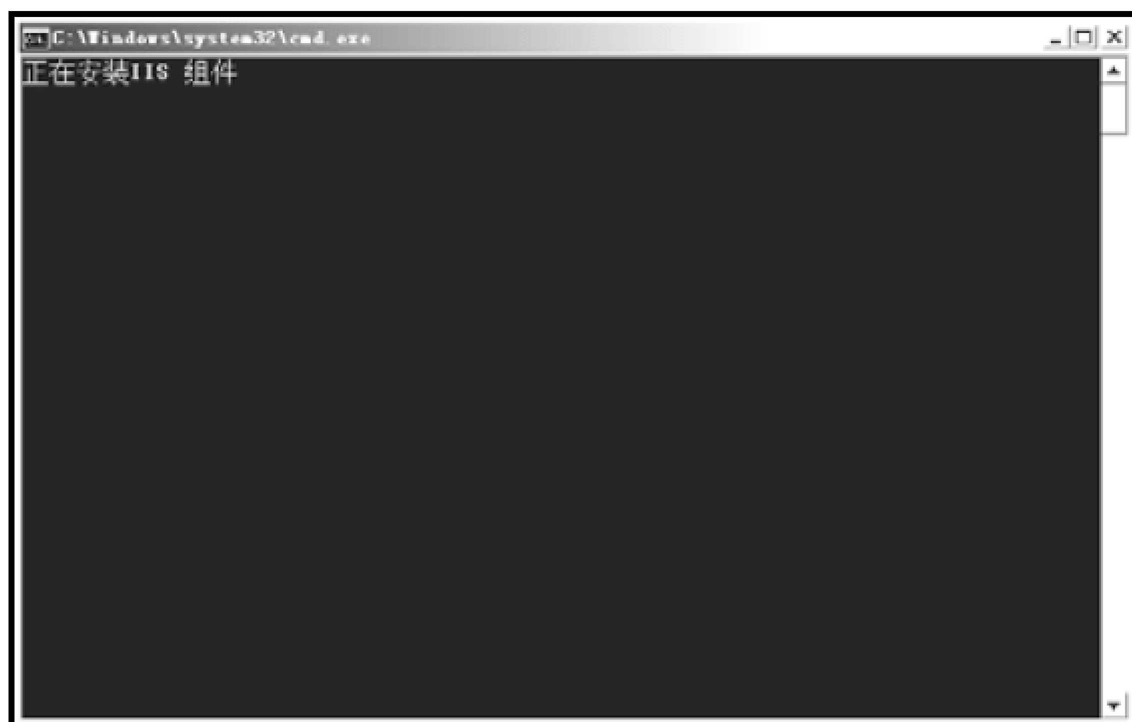


图 8-25　IIS 组件安装对话框



图 8-26　U-Mail Mail Server 安装向导对话框

03 弹出【许可证协议】对话框，选中【我接受“许可证协议”中的条款】复选框，单击【下一步】按钮，如图 8-27 所示。

04 弹出【系统需安装的组件】对话框，默认选择所有组件，单击【下一步】按钮，如图 8-28 所示。

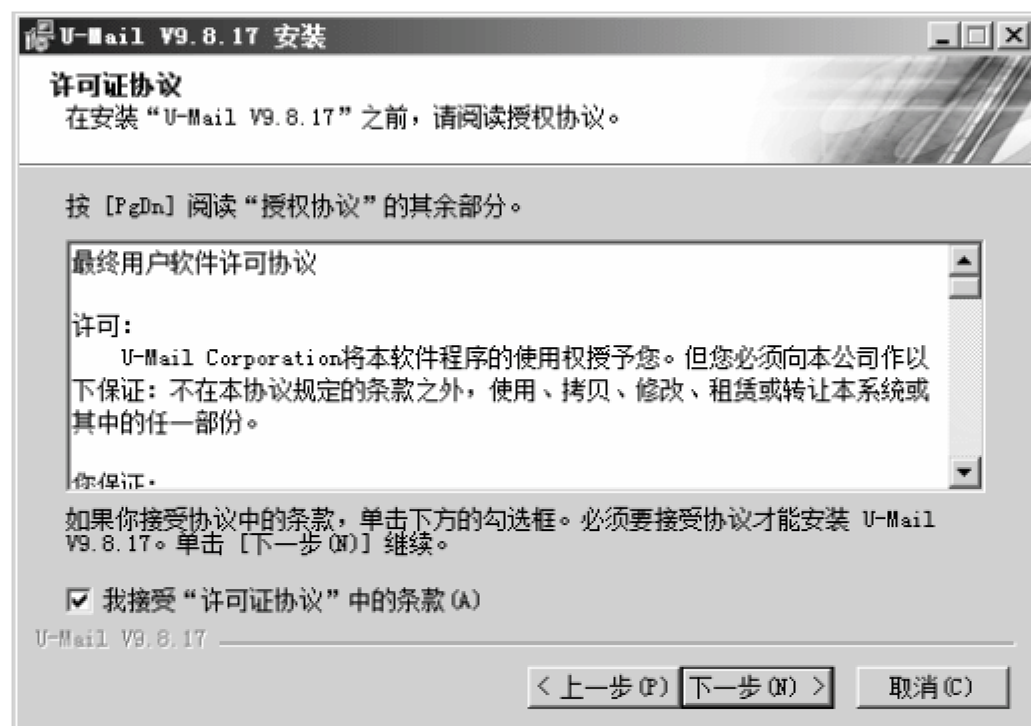


图 8-27　【许可证协议】对话框

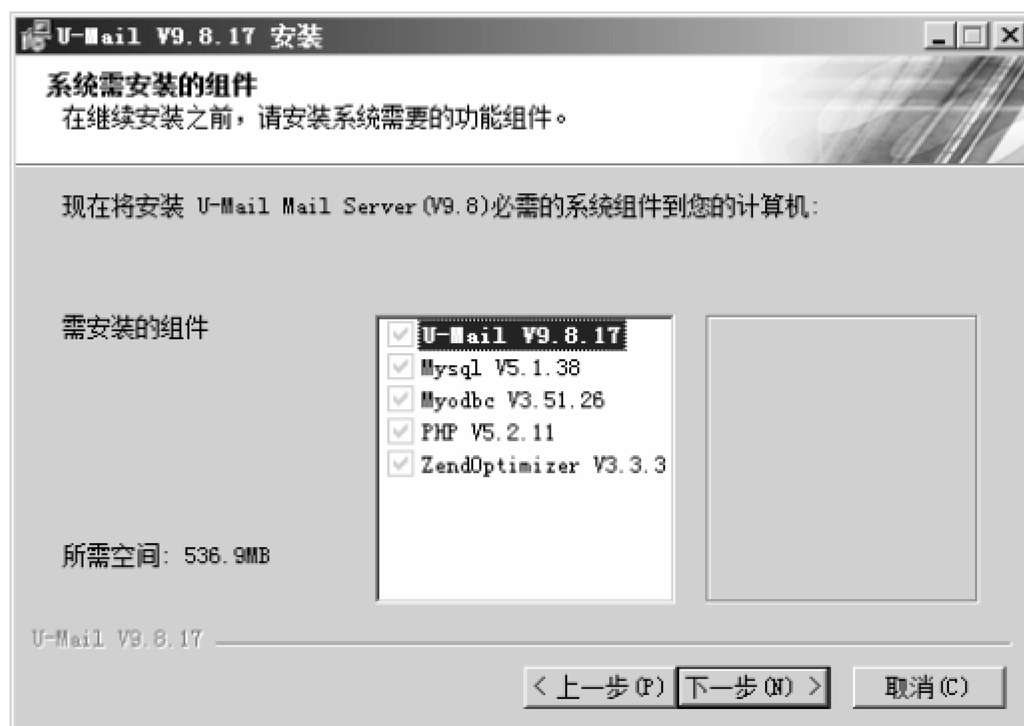


图 8-28　【系统需安装的组件】对话框

05 弹出【选定安装位置】对话框，在【目标文件夹】文本框中输入安装目录，也可以单击

【浏览】按钮选择安装目录，本实例采用默认值，单击【下一步】按钮，如图 8-29 所示。

06 弹出【U-Mail 邮件系统主域名设置】对话框，在【域名】文本框中输入企业申请的将要使用的邮箱域名，在【本地 IP 地址】文本框中输入 U-Mail 服务器的 IP 地址，在【IIS 端口】文本框中输入 Web 访问邮件服务器使用的端口，本实例全部采用默认配置，单击【下一步】按钮，如图 8-30 所示。

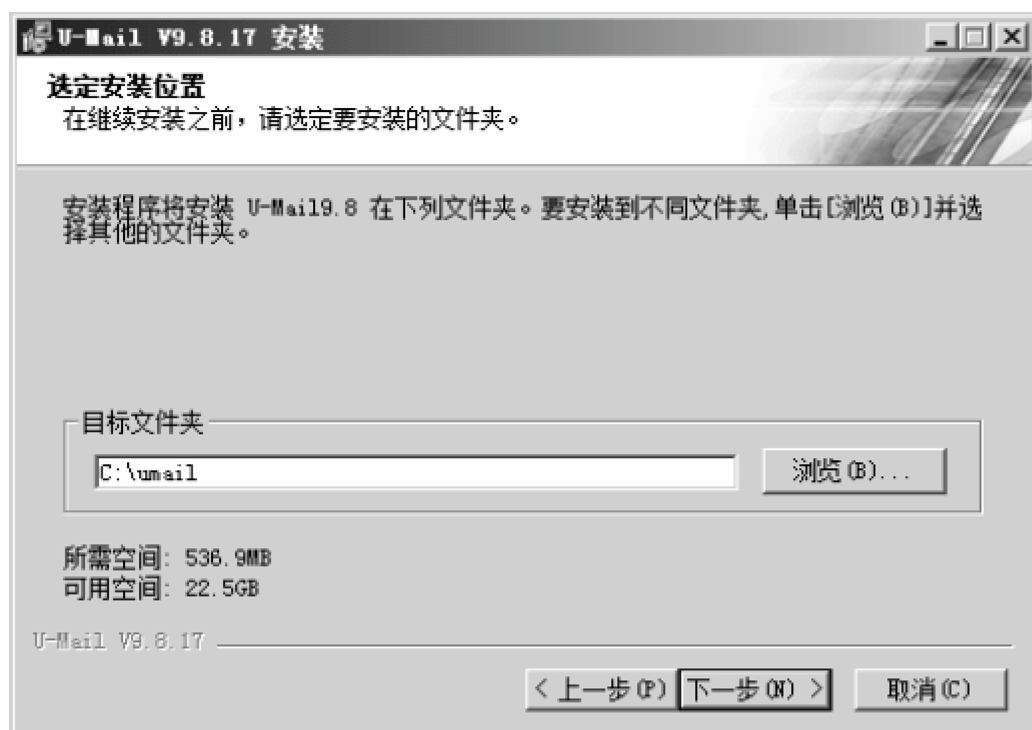


图 8-29 【选定安装位置】对话框

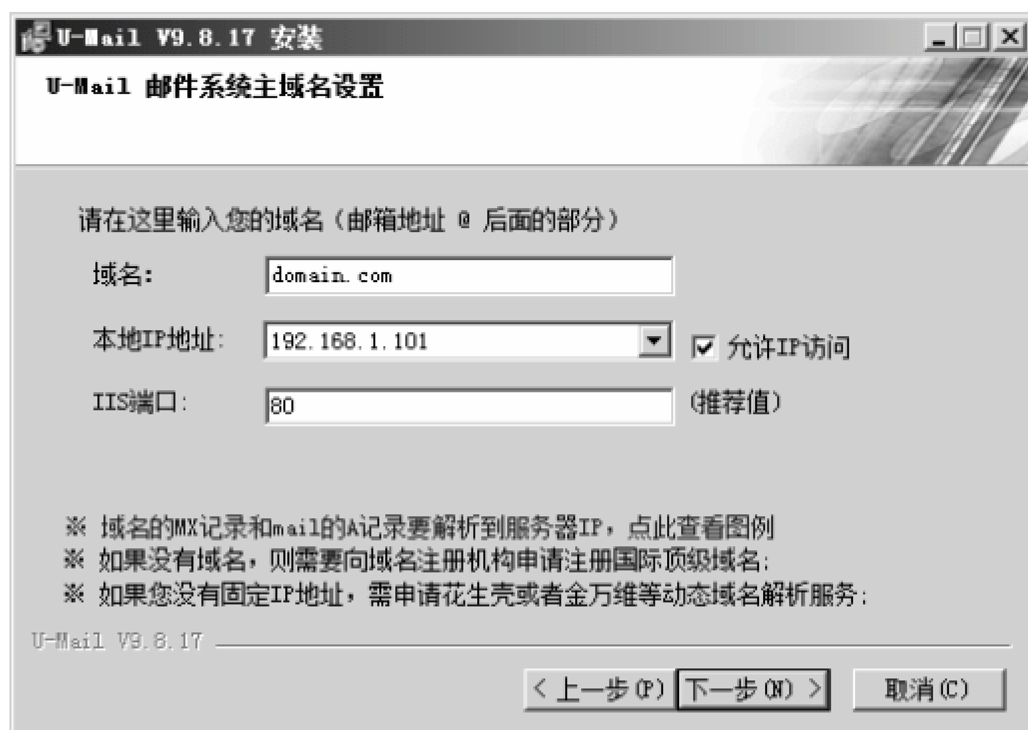


图 8-30 【U-Mail 邮件系统主域名设置】对话框

07 弹出【U-Mail 邮件系统管理账号设置】对话框，在三个文本框中分别输入不同管理账号使用的访问密码，密码要求具有一定的复杂性，且尽量不要使用同一密码，单击【下一步】按钮，如图 8-31 所示。

08 弹出【开始安装】对话框，单击【安装】按钮，如图 8-32 所示。

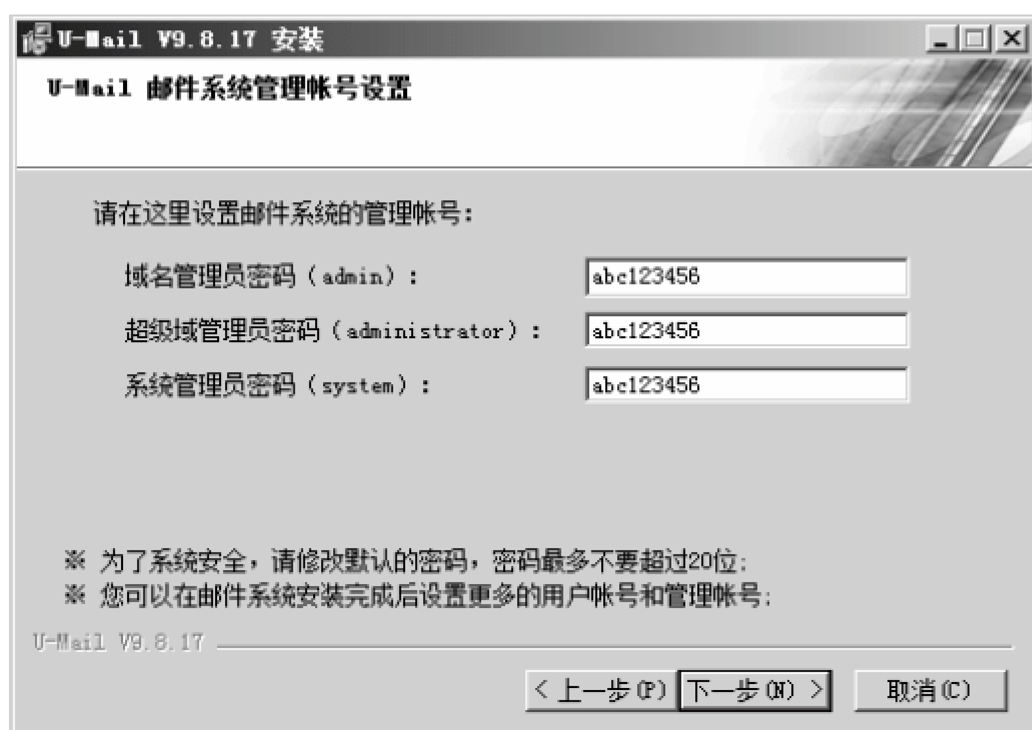


图 8-31 【U-Mail 邮件系统管理账号设置】对话框

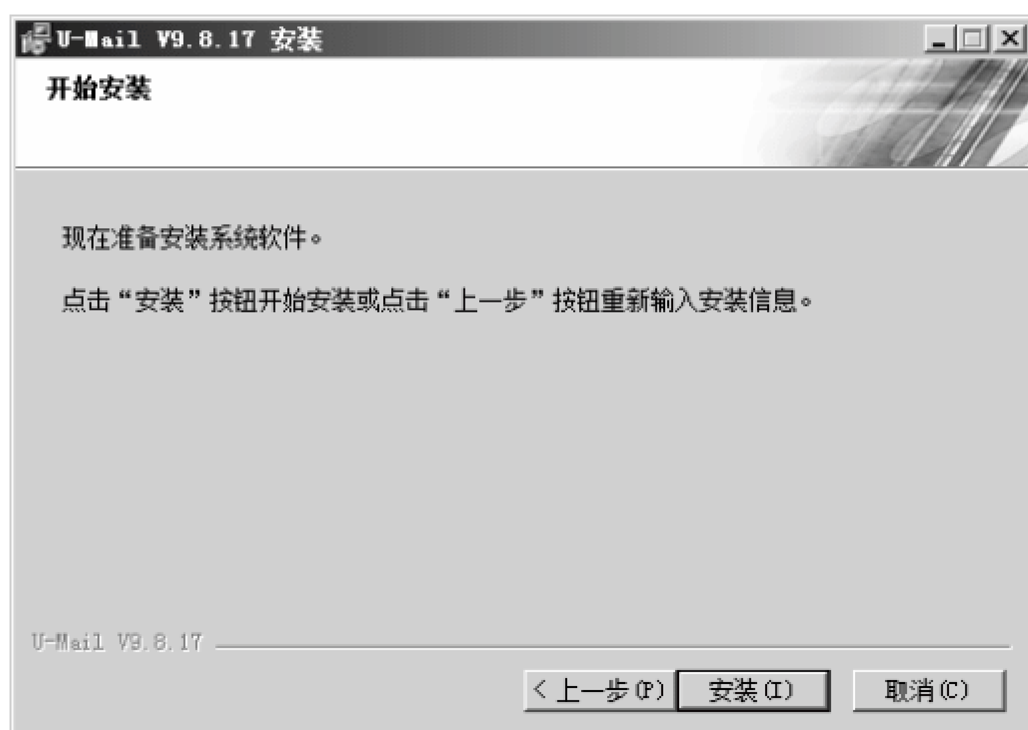


图 8-32 【开始安装】对话框

09 弹出【正在安装】对话框，系统自动安装程序，并显示安装进度，如图 8-33 所示。

10 安装完成后，弹出【邮件系统更新参数设置】对话框，采用默认配置，单击【下一步】按钮，如图 8-34 所示。



图 8-33　【正在安装】对话框

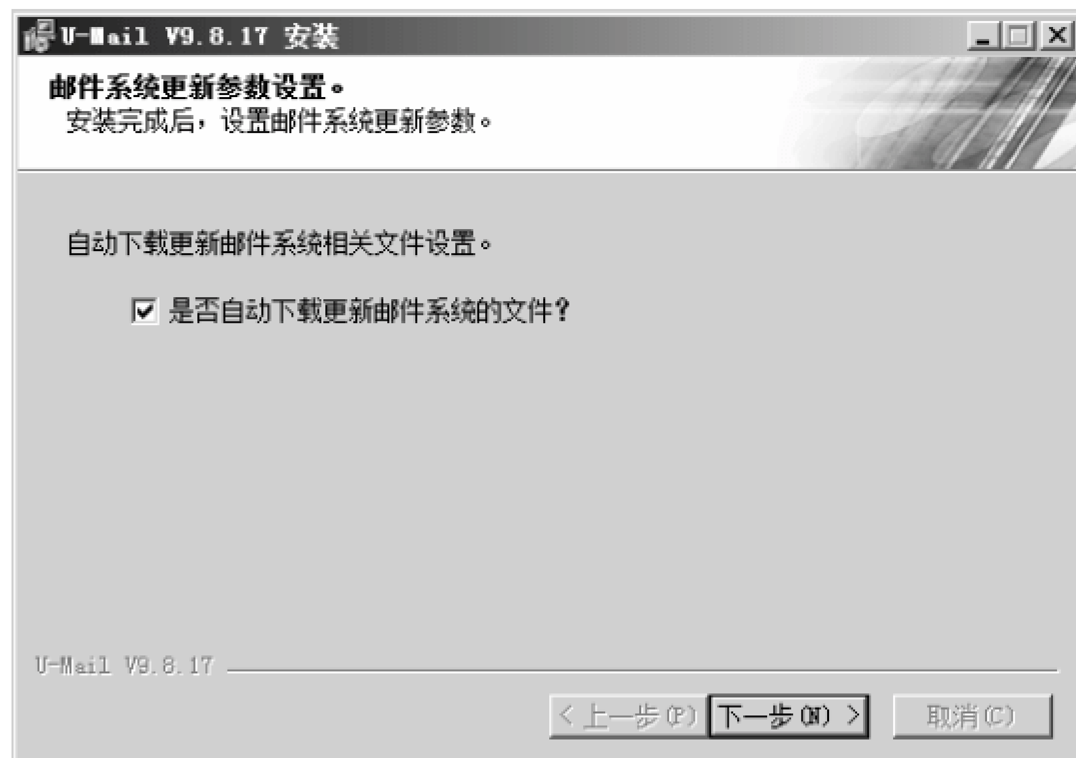


图 8-34　【邮件系统更新参数设置】对话框

11 U-Mail 邮件服务器安装完成，单击【完成】按钮结束安装向导，如图 8-35 所示。

12 弹出系统重启提示框，单击【是】按钮，重启系统使 U-Mail 服务生效，如图 8-36 所示。

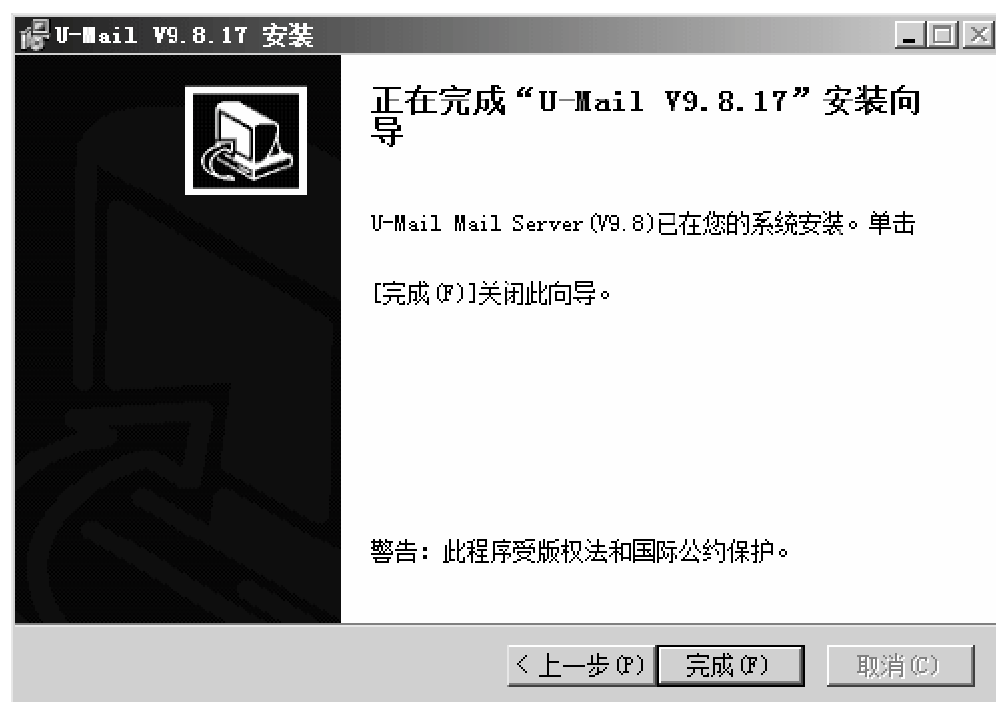


图 8-35　U-Mail 安装向导完成对话框

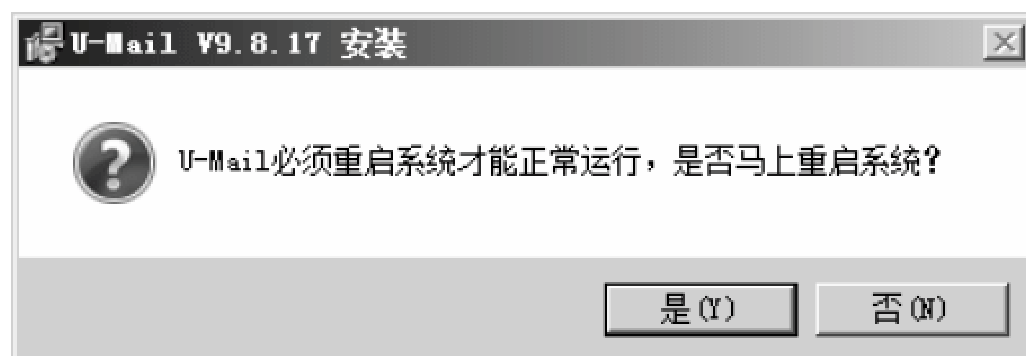
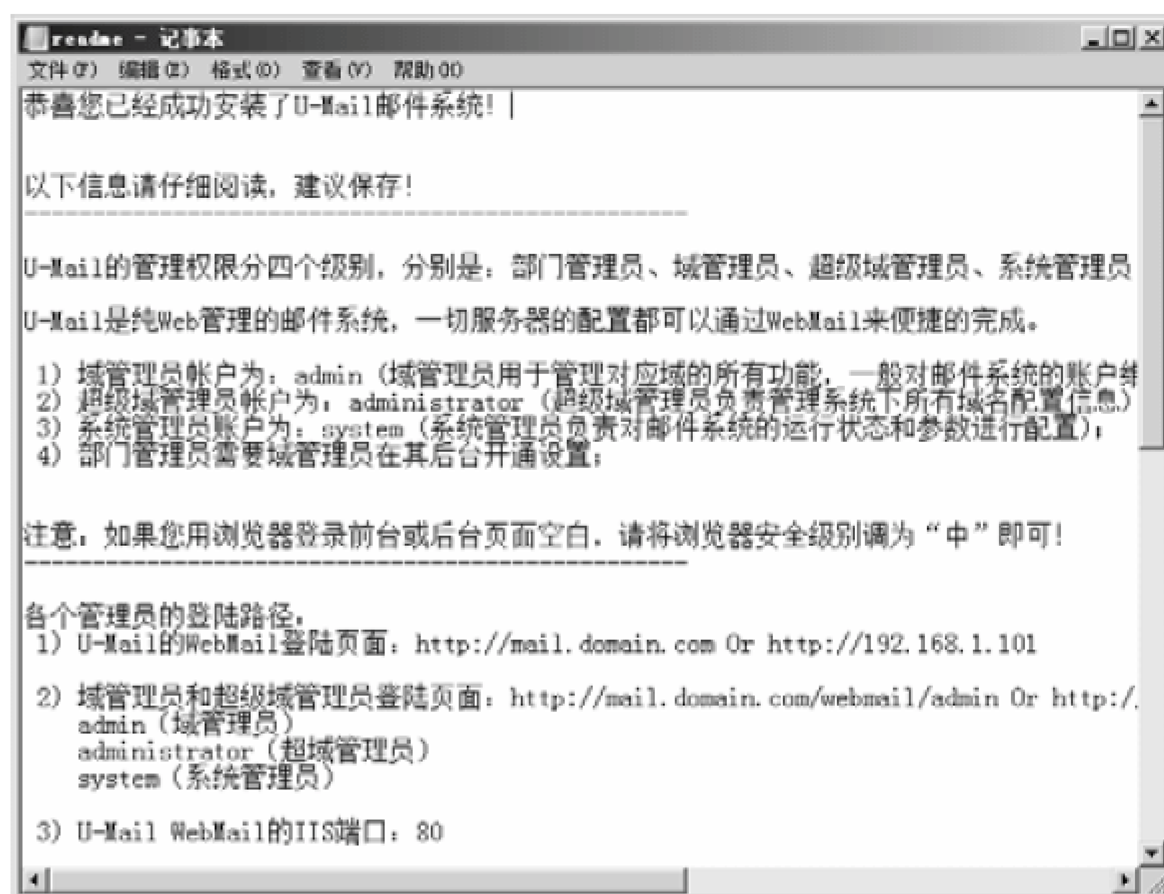


图 8-36　系统重启提示框

13 安装完成后，在系统桌面自动生成文本文件"readme"，该文件简单介绍了 U-Mail 邮件服务器的管理方法，包括 Web 管理地址以及不同级别账户的访问名与管理职能等信息。建议管理员妥善保存，如图 8-37 所示。


readme - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

恭喜您已经成功安装了U-Mail邮件系统!

以下信息请仔细阅读，建议保存!

U-Mail的管理权限分四个级别，分别是：部门管理员、域管理员、超级域管理员、系统管理员

U-Mail是纯Web管理的邮件系统，一切服务器的配置都可以通过WebMail来便捷的完成。

1) 域管理员帐户为：admin（域管理员用于管理对应域的所有功能，一般对邮件系统的账户维
2) 超级域管理员帐户为：administrator（超级域管理员负责管理系统下所有域名配置信息）
3) 系统管理员账户为：system（系统管理员负责对邮件系统的运行状态和参数进行配置）；
4) 部门管理员需要域管理员在其后台开通设置；

注意：如果您用浏览器登录前台或后台页面空白，请将浏览器安全级别调为"中"即可!

各个管理员的登陆路径：
1) U-Mail的WebMail登陆页面：http://mail.domain.com Or http://192.168.1.101

2) 域管理员和超级域管理员登陆页面：http://mail.domain.com/webmail/admin Or http:/
admin（域管理员）
administrator（超域管理员）
system（系统管理员）

3) U-Mail WebMail的IIS端口：80

图 8-37　U-Mail 邮件系统成功安装说明文件

8.2.4　使用管理账户配置邮件服务器

在 U-Mail 邮件服务器中提供了三种管理账户，分别是域管理员、超域管理员、系统管理员，这三个账户可以分别完成不同的管理职能。下面将分别配置三种管理权限下的不同服务内容。

1. 域管理员

域管理员主要可以进行邮箱账户的添加与管理，邮件的监管，以及 Web mail 定制。使用域管理员管理邮件服务器的具体操作内容如下。

01 启动 U-Mail 服务器，右击任务栏通知区域的 U-Mail 服务图标，弹出快捷菜单，选择【域管理后台】命令，如图 8-38 所示。

02 弹出【企业邮箱管理登录】页面，在【管理员类别】下拉列表中选择【域管理员】，在【用户名】和【密码】文本框中分别输入域管理员的账号和密码，单击【登录】按钮，如图 8-39 所示。

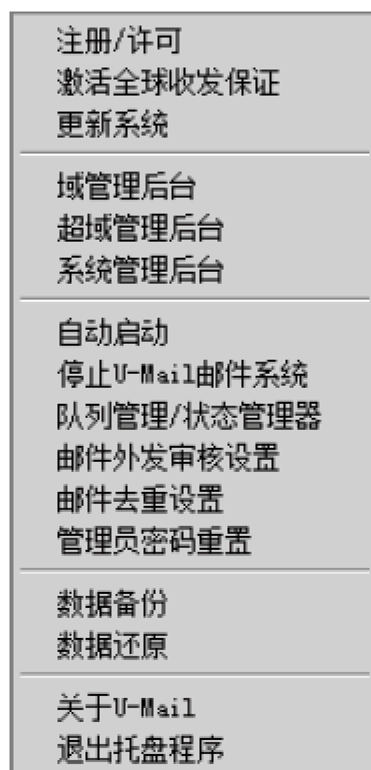


图 8-38　U-Mail 邮件系统快捷菜单



图 8-39　U-Mail 邮件系统属性

03 打开【“企业邮局”邮件系统域管理后台】页面，默认显示【域信息管理统计】和【注册企业基本信息】，读者可以自行查看或配置相关内容，如图 8-40 所示。



图 8-40　【域信息管理统计】界面

04 在左侧列表中选择【邮件管理】➢【添加新用户】选项，显示【添加邮箱账户】页面，通过该页面可以为员工创建邮箱账户，如图 8-41 所示。

图 8-41 【添加邮箱账户】页面

05 如果员工比较多，一个个地创建会很麻烦，可以选择【邮件管理】➢【批量添加用户】选项，在右侧的【批量添加用户】页面中批量创建账户。批量创建账户的方法页面中有详细的介绍，如图 8-42 所示。

图 8-42 【批量添加用户】页面

有关域管理员的其他内容本书不作介绍，读者可以自行安装学习。

2. 超域管理员

使用超域管理员登录后可以完成邮件域的管理，同时也可以完成域管理员的大部分工作。使用超域管理员创建新域的具体操作步骤如下。

01 启动 U-Mail 服务器，右击任务栏通知区域的 U-Mail 服务图标，弹出快捷菜单，选择【超域管理后台】命令，如图 8-43 所示。

02 打开【企业邮箱管理登录】页面，在【管理员类别】下拉列表中选择【域管理员】，在【用户名】和【密码】文本框中分别输入超域管理员的账号和密码，单击【登录】按钮，如图 8-44 所示。

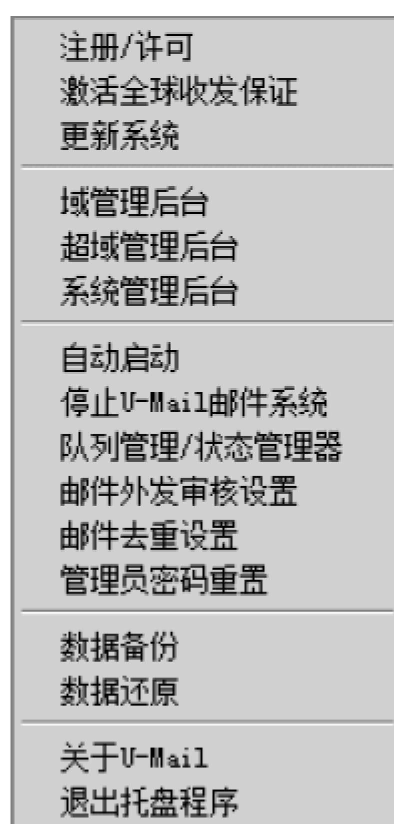


图 8-43　U-Mail 邮件系统快捷菜单



图 8-44【企业邮箱管理登录】对话框

03 打开【U-Mail 超域管理后台】页面，该页面主要包括【企业邮局基本信息】和【注册企业基本信息】，读者可以根据需求自行设置，设置完成后单击【修改】按钮使其生效，如图 8-45 所示。



图 8-45　【U-Mail 超域管理后台系统】页面

04 在左侧列表中选择【邮件域管理】➢【添加域名】选项，可以为邮箱创建新的域名后缀，并制定新域名后缀邮箱的相关配置内容，设置完成后单击【提交】按钮，如图 8-46 所示。



图 8-46 【添加域名】页面

3. 系统管理员

01 启动 U-Mail 服务器，右击任务栏通知区域的 U-Mail 服务图标，弹出快捷菜单，选择【系统管理后台】命令，如图 8-47 所示。

02 打开【系统管理员登录】页面，在【电子邮件地址】和【密码】文本框中分别输入系统管理员的账号和密码，单击【登录】按钮，如图 8-48 所示。

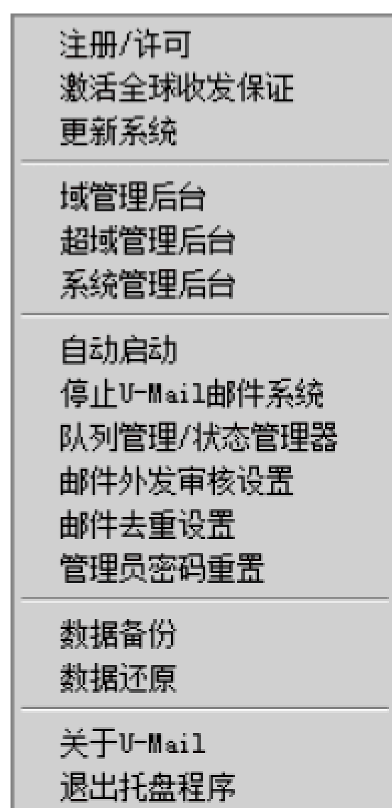


图 8-47 U-Mail 邮件系统快捷菜单



图 8-48 【系统管理员登录】页面

03 打开系统管理员的管理页面，默认显示邮件服务器的当前状态，包括服务器运行状态、

U-Mail 统计等内容，如图 8-49 所示。



图 8-49　系统管理员主菜单窗口

04 选择左侧的【域】选项，在右侧显示当前邮件服务器可用的域名，选择域名后可单击【编辑】按钮，如图 8-50 所示。

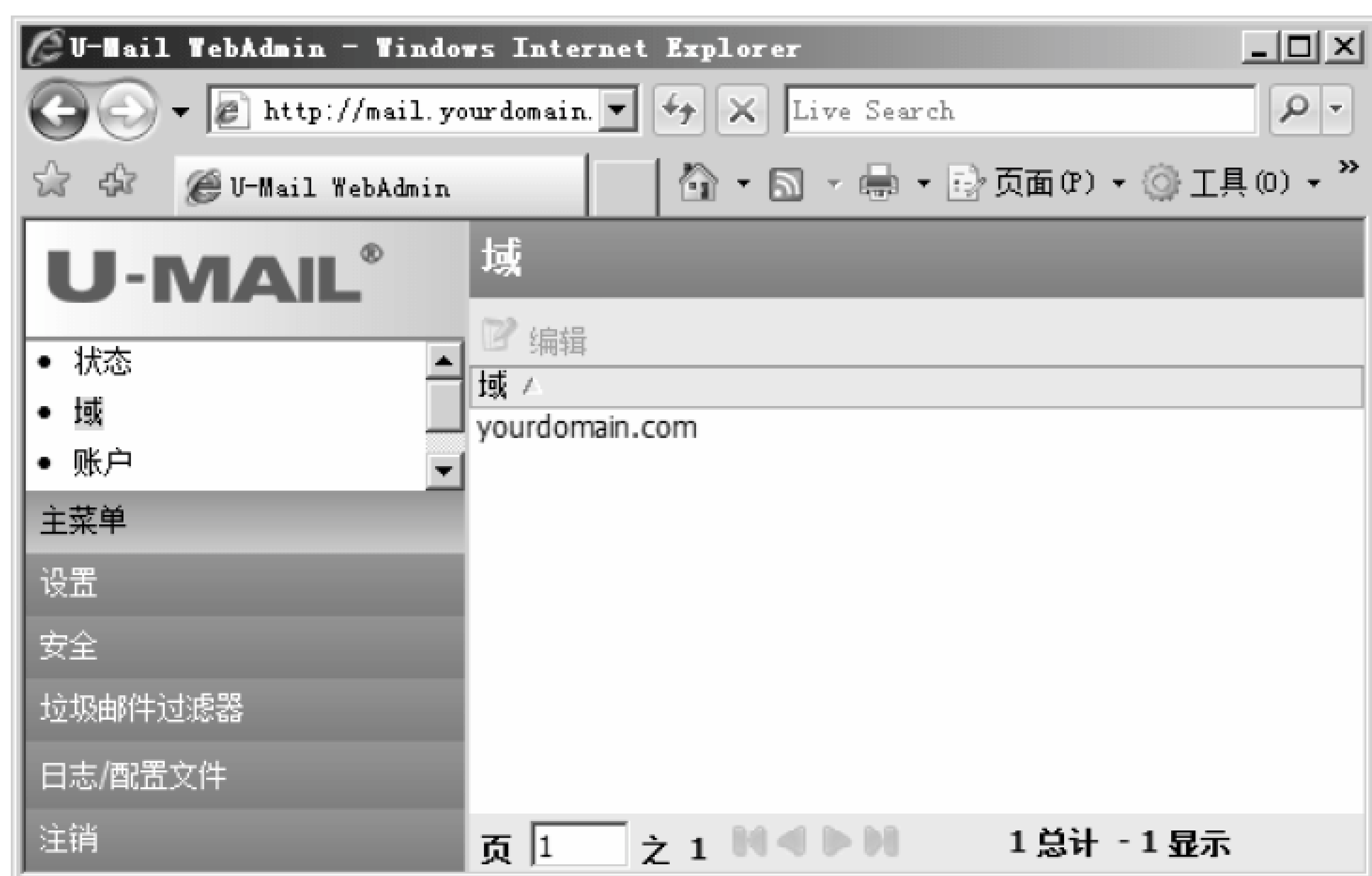


图 8-50　系统管理员登录域名窗口

05 打开域的编辑页面，可以编辑域的【属性】和【用户】信息，属性中【IP 地址】文本框应该输入邮件服务器的 IP 地址，配置完成后单击左上角的【保存】按钮，如图 8-51 所示。



图 8-51　域的编辑页面

06 返回系统管理员的管理页面，在左侧窗格中选择【账户】选项，右侧窗格显示当前邮件服务器的账户信息，如图 8-52 所示，显示了 3 个已创建的账户，选择一个账户，单击【编辑】按钮，可对该账户进行设置。

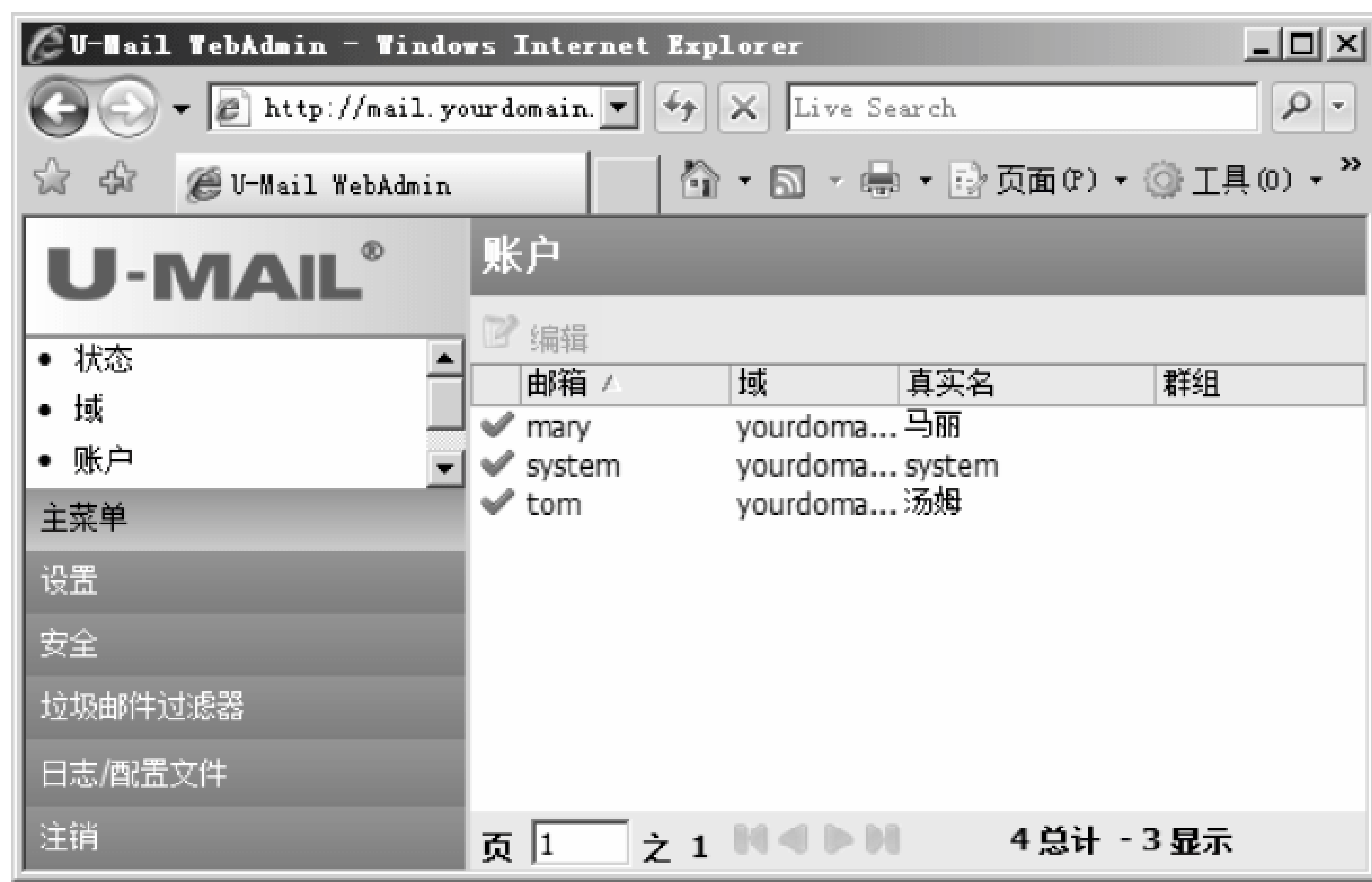


图 8-52　系统管理员的账户管理页面

系统管理员管理页面左侧的其他选项在下文中进行介绍。

8.2.5　为企业员工分配邮件账户

使用 U-Mail 为企业员工分配邮件账户时，主要由管理员操作，在此为员工马丽分配邮件账户，具体操作步骤如下。

01 打开【企业邮箱管理登录】页面，在【用户名】和【密码】文本框中分别输入超域管理

员的账户及密码，单击【登录】按钮，如图 8-53 所示。



图 8-53　【企业邮箱管理登录】页面

02 打开【“企业邮局”邮件系统域管理后台】页面，在左侧列表中选择【邮件管理】➢【添加新用户】，弹出【添加邮箱账户】对话框，用户名为“mary”，密码为“123456mary”，依次进行填写，账户名称、登录密码、确认密码、邮箱容量、网络硬盘容量、邮箱收发权限、真实姓名等相关信息，最后单击【添加】按钮，如图 8-54 所示。若要为其他用户分配邮件账户，步骤同上。



图 8-54　【添加邮箱账户】页面

03 打开 IE 浏览器，在地址栏输入“http://mail.yourdomain.com”，进入 U-Mail 的 Web Mail 登录页面，在【登录账号】和【登录密码】文本框中输入“mary”和“123456mary”，单击【登录】按钮，如图 8-55 所示。



图 8-55 【登录企业邮箱】页面

04 进入收发邮件界面，单击【写信】按钮，在此进行编辑和发送邮件，如图 8-56 所示。该邮箱的其他操作内容和通用的互联网邮箱相似。

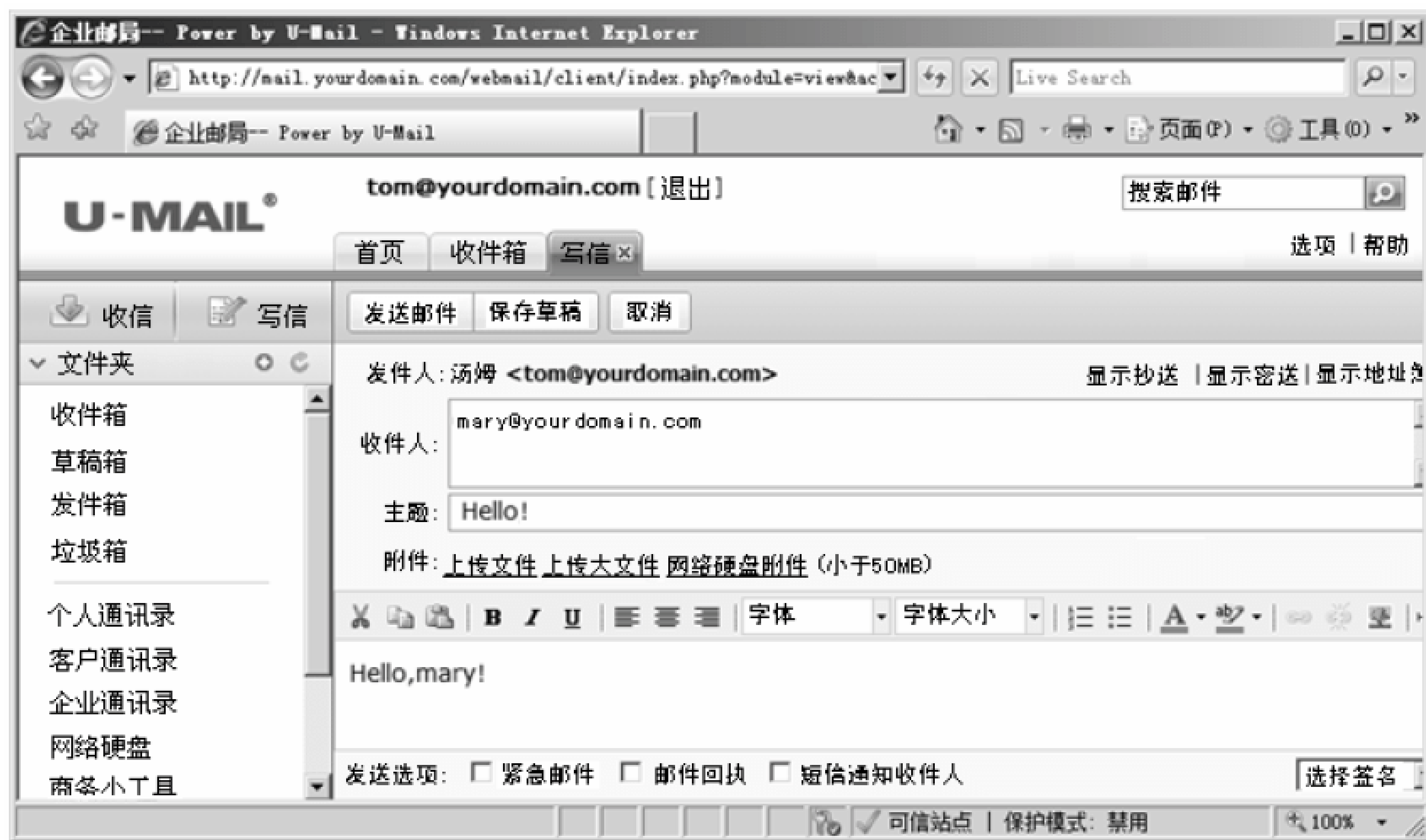


图 8-56 用户邮箱界面

8.2.6 反垃圾邮件和个人邮箱限制

垃圾邮件猖獗，作为管理员必须要对其进行防护，U-Mail 服务器有非常好的反垃圾邮件设置，具体操作方法如下。

01 使用系统管理员登录，进入系统管理后台页面，在左侧选择【垃圾邮件过滤器】选项，在上面弹出相应子菜单选项，选择【垃圾邮件过滤器】选项，右侧弹出【垃圾邮件过滤器－启发式】页面，在启发式引擎选项中采取默认设置即可，如图 8-57 所示。

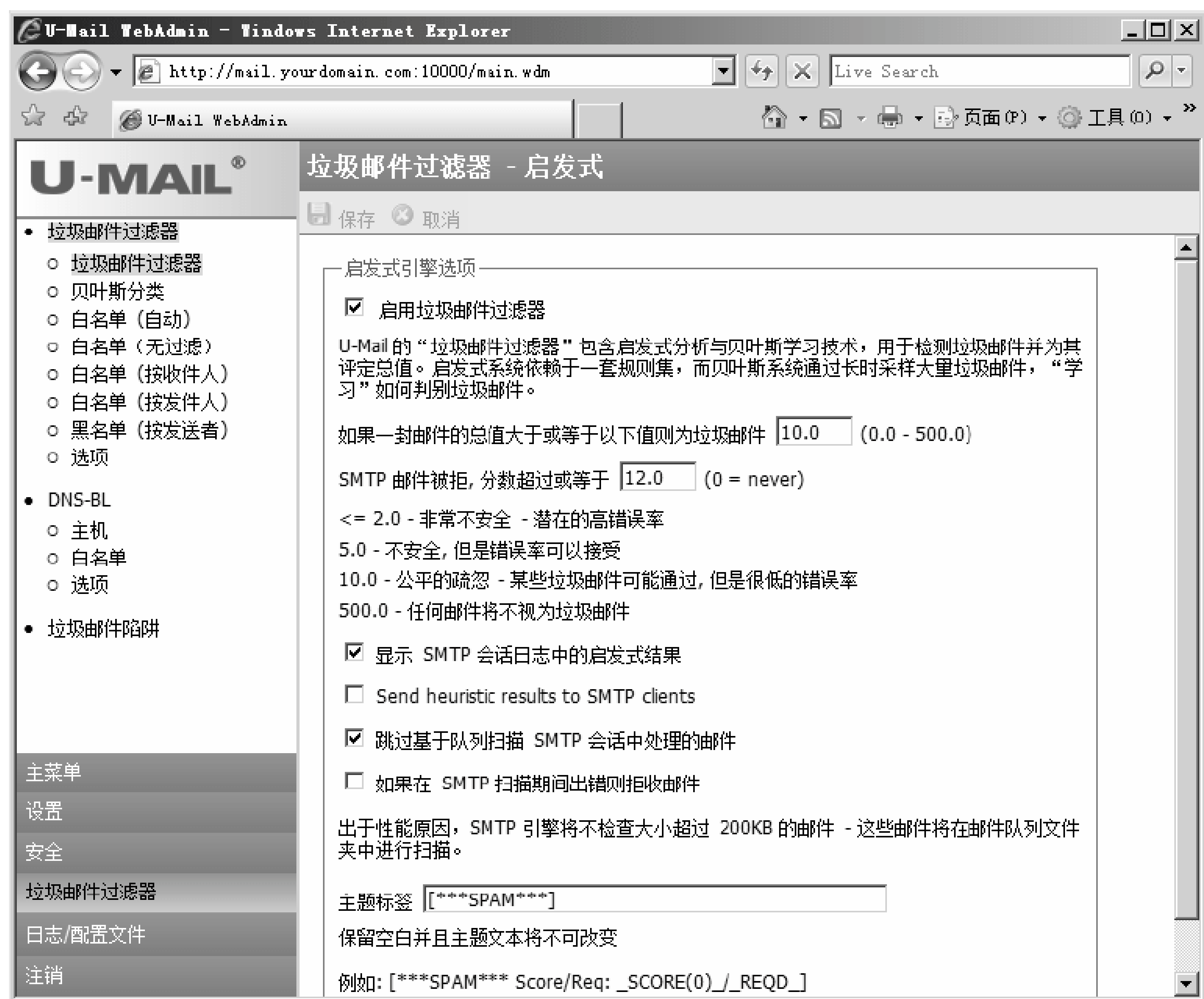


图 8-57 【垃圾邮件过滤器－启发式】页面

02 选择【垃圾邮件过滤器】➢【垃圾邮件过滤器】➢【白名单（无过滤）】选项，这里是排除发送到对方的地址不进行反垃圾过滤。例如，发送到 comingchina.com 的邮件不进行过滤，则在编辑框里输入“*@comingchina.com”，如图 8-58 所示。



图 8-58 【垃圾邮件过滤器－白名单】编辑框

03 选择【垃圾邮件过滤器】➢【垃圾邮件过滤器】➢【黑名单（按发送者）】命令，这里设置好某个地址，则这个发过来的邮件都将被列为垃圾邮件。前面的#号是注释符，如需要添加不

用加#，如图 8-58 所示。

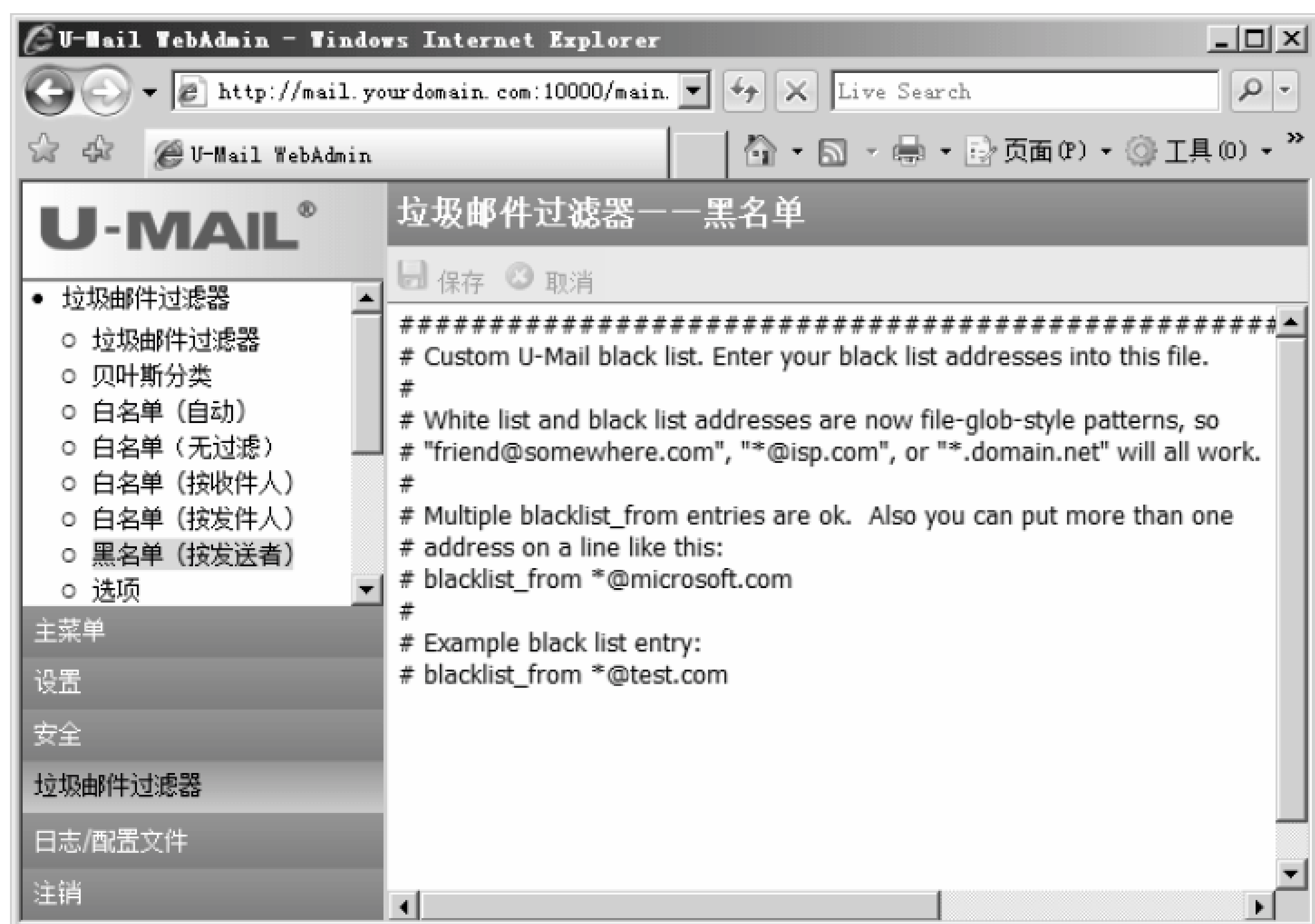


图 8-59 【垃圾邮件过滤器－黑名单】编辑框

04 选择【垃圾邮件过滤器】➢【垃圾邮件过滤器】➢【白名单（按发件人）】命令，在弹出的编辑框中排除外面发进来的邮件不进行垃圾邮件过滤。例如，排除 abc.com 发过来的邮件不进行垃圾邮件过滤，则在编辑框里输入“whitelist_from*@abc.com”，如图 8-60 所示。

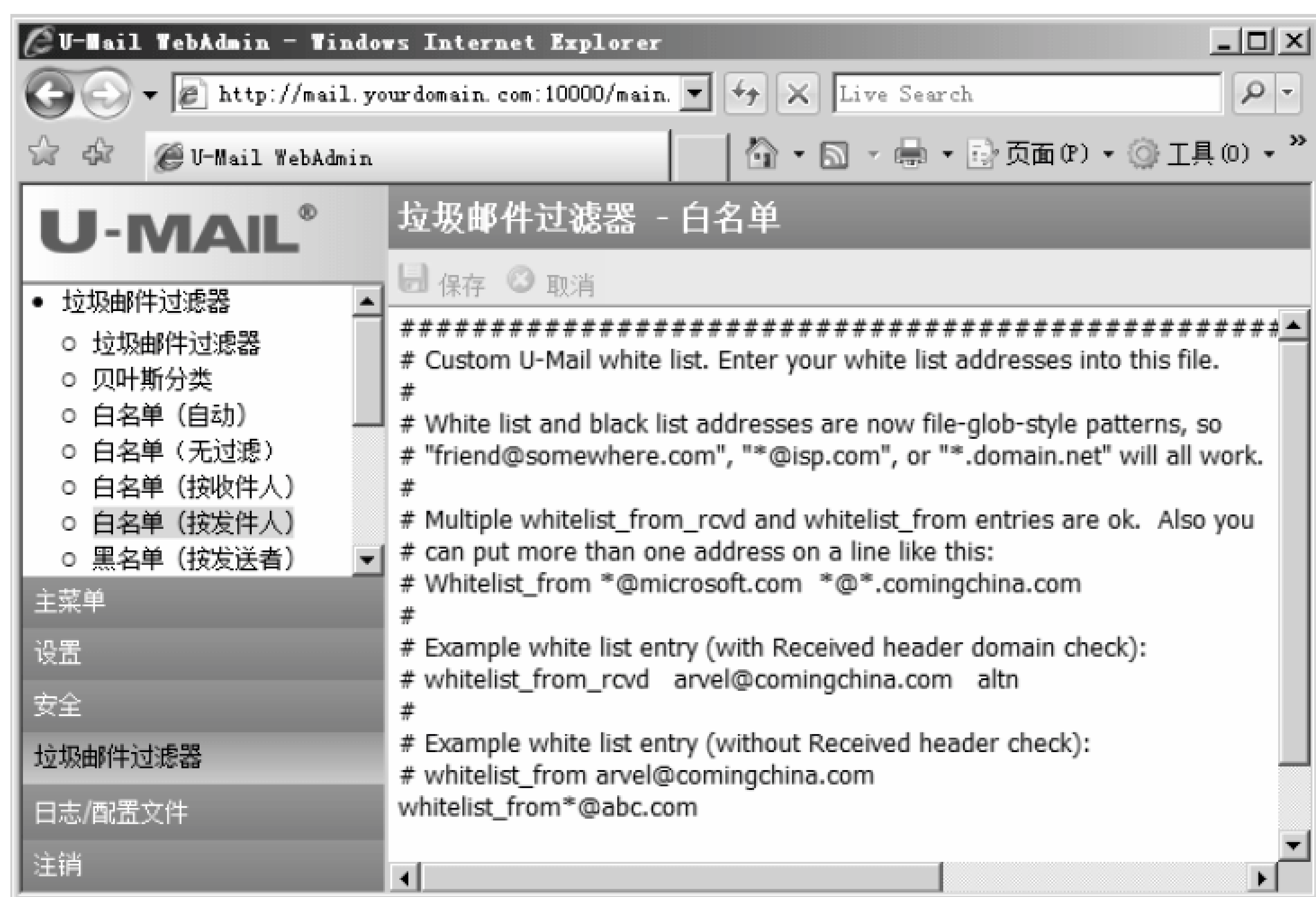


图 8-60 【垃圾邮件过滤器－白名单】编辑框

05 选择【垃圾邮件过滤器】➢【垃圾邮件过滤器】➢【白名单（按收件人）】选项，在弹出的编辑框中排除本地某个邮箱或者服务器的某个域名不进行垃圾邮件过滤，如图 8-61 所示。

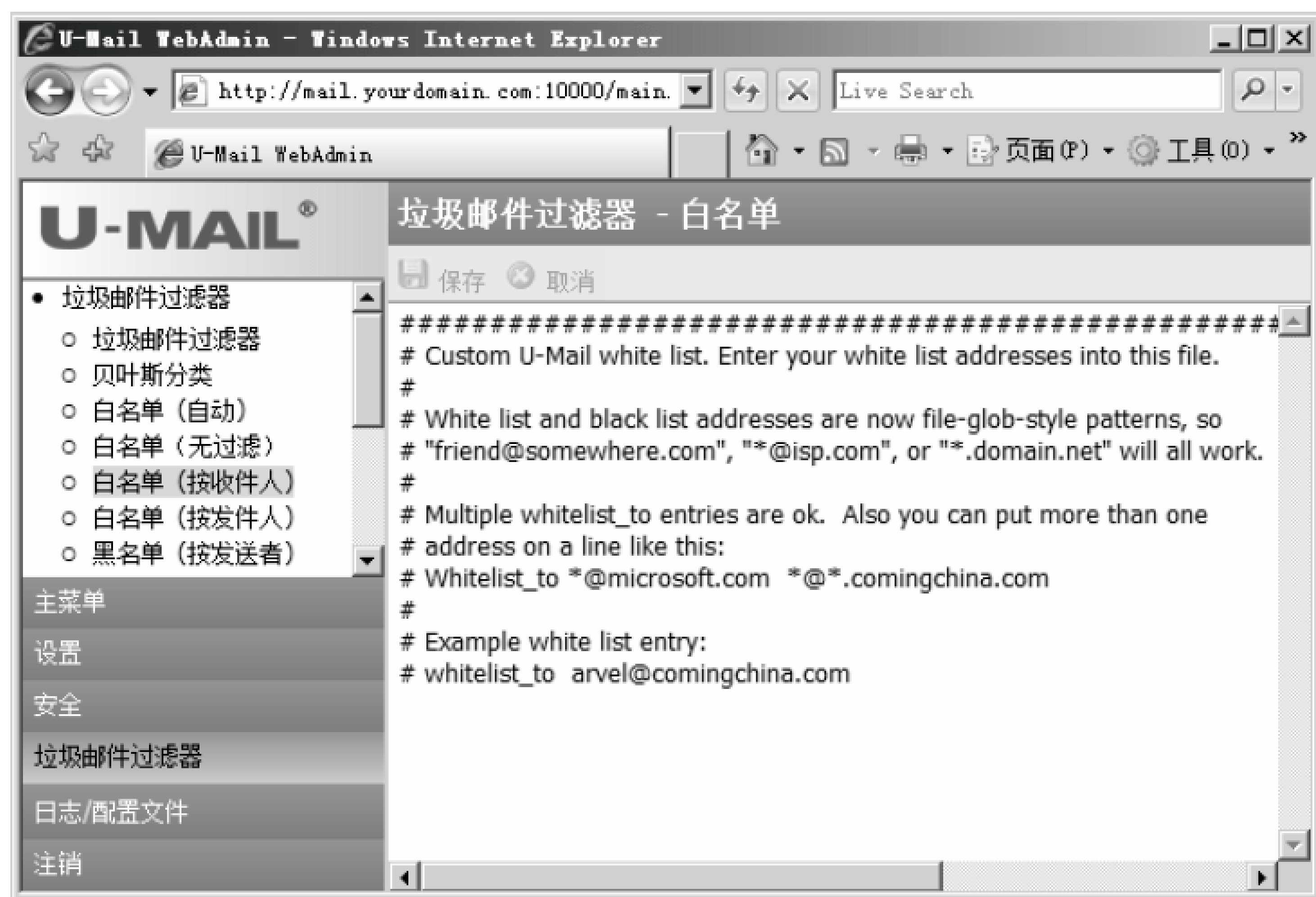


图 8-61　【垃圾邮件过滤器—白名单（按收件人）】编辑框

06 启动 U-Mail 服务器，选择【超域管理后台】➢【邮箱管理】➢【邮箱用户管理】命令，弹出【邮箱用户列表】页面，选择用户“马丽”，单击【操作】列里的【修改】链接，如图 8-62 所示。



图 8-62　【邮箱用户管理】页面

07 进入【修改邮箱账户】页面，对用户邮箱容量进行限制设定，如图 8-63 所示。



图 8-63 【修改邮箱账户】对话框

8.3 专家答疑

（1）搭建邮件服务器是否必须要固定 IP？

答：是否需要固定 IP，主要取决于实际需要。一般来讲，固定 IP 要比动态 IP 稳定得多，在预算许可的情况下，建议最好使用动态 IP，不过如果用户数不是很多，邮件量不是很大，预算也不许可，那么使用动态 IP 对于 U-Mail 来讲是没有什么差别的，U-Mail 都会尽可能达到一定的送达率。一般来讲用户数不超过 500 用户数，使用动态 IP，影响不是很大。

（2）Web mail 安全性怎么样？

答：Web mail 使用定制的 PHP+MySQL，安全性好，效率高；支持数字证书服务并提供强大的管理功能，可直接在 Web mail 中撰写或阅读经过数字签名/加密的安全邮件（S/MIME）。提供军事级别的高安全强度（4096 位 DH/DSS 加密或 2048 位 RSA 加密）；使用 TLS/SSL 标准安全套接字层通信协议（1024 位 RSA 加密），支持包括 SSL SMTP、SSL POP3、SSL IMAP4 安全通信服务，防止网络侦听，使得通信更安全。

第 9 章　企业网站的搭建与维护

为了更好地对外宣传，现在很多公司都建立了自己的网站，如何更好地更新和维护网站，就成了公司宣传的重要组成部分，下面主要讲解基于 IIS 的网站发布技术。

9.1　企业网站管理概述

企业网站主要是商业宣传性网站，为了保障网站的正常运行，必须选择一个性能良好的网站发布工具，为网站的良好运行做好各种准备。下面主要介绍 IIS 和搭建企业网站环境需要做的准备工作。

9.1.1　IIS 介绍

IIS（Internet Information Services，因特网信息服务），是由微软公司提供的基于运行 Microsoft Windows 的互联网基本服务。IIS 可以用做架设网站、FTP 服务器、SMTP 服务器、NNTP 服务器等，目前在 Windows Server 2003 系统上可以安装的为 IIS6.0 版本，在 Windows Server 2008 系统上可以安装的为 IIS7.0 版本。

9.1.2　搭建企业网站环境的准备工作

默认情况下，Windows Server 2008 并不会安装 IIS，需要网络管理人员进行手工安装，不过在安装之前有一些准备工作需要做。

（1）如果说要通过域名来访问网站，需要在域名运营商处注册域名。

（2）IIS 服务器的计算机最好设置为固定 IP 地址，这样既方便用户访问又方便服务器管理。

（3）IIS 服务器网页数据的保存，IIS 服务器的分区最好为 NTFS 分区，因为 NTFS 文件系统能够很好地保证数据的安全性。

（4）网站如要进行 SSL 安全连接，需要向 CA 申请网站证书。

9.2　项目实战 1：搭建企业网站环境

IIS 是 Windows 系统上市场份额最多的网站发布组件，目前最为流行的为 IIS7.0 版本。下面详

细讲解如何安装 IIS 组件，以及如何在 Web 服务器上发布第一个网站。

9.2.1 安装 Web 服务器（IIS 组件）

和 Windows Server 2003 相比，Windows Server 2008 将各种服务归类为角色，通过添加 IIS 服务角色来安装 IIS 组件，具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，选择左侧【角色】选项，如图 9-1 所示，在右侧选择【添加角色】选项。

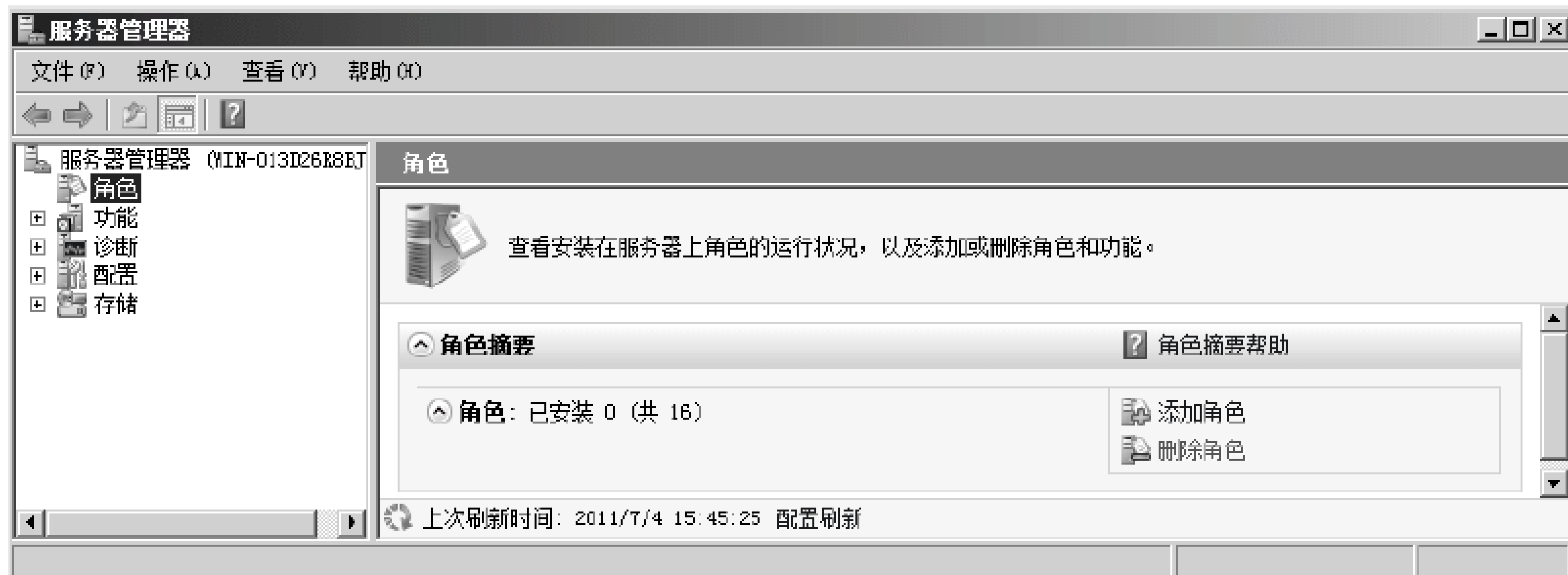


图 9-1 【服务器管理器】窗口

02 弹出【添加角色向导】对话框，如图 9-2 所示，单击【下一步】按钮。

03 弹出【添加服务器角色】对话框，如图 9-3 所示，选中【Web 服务器（IIS）】复选框。



图 9-2 【添加角色向导】对话框

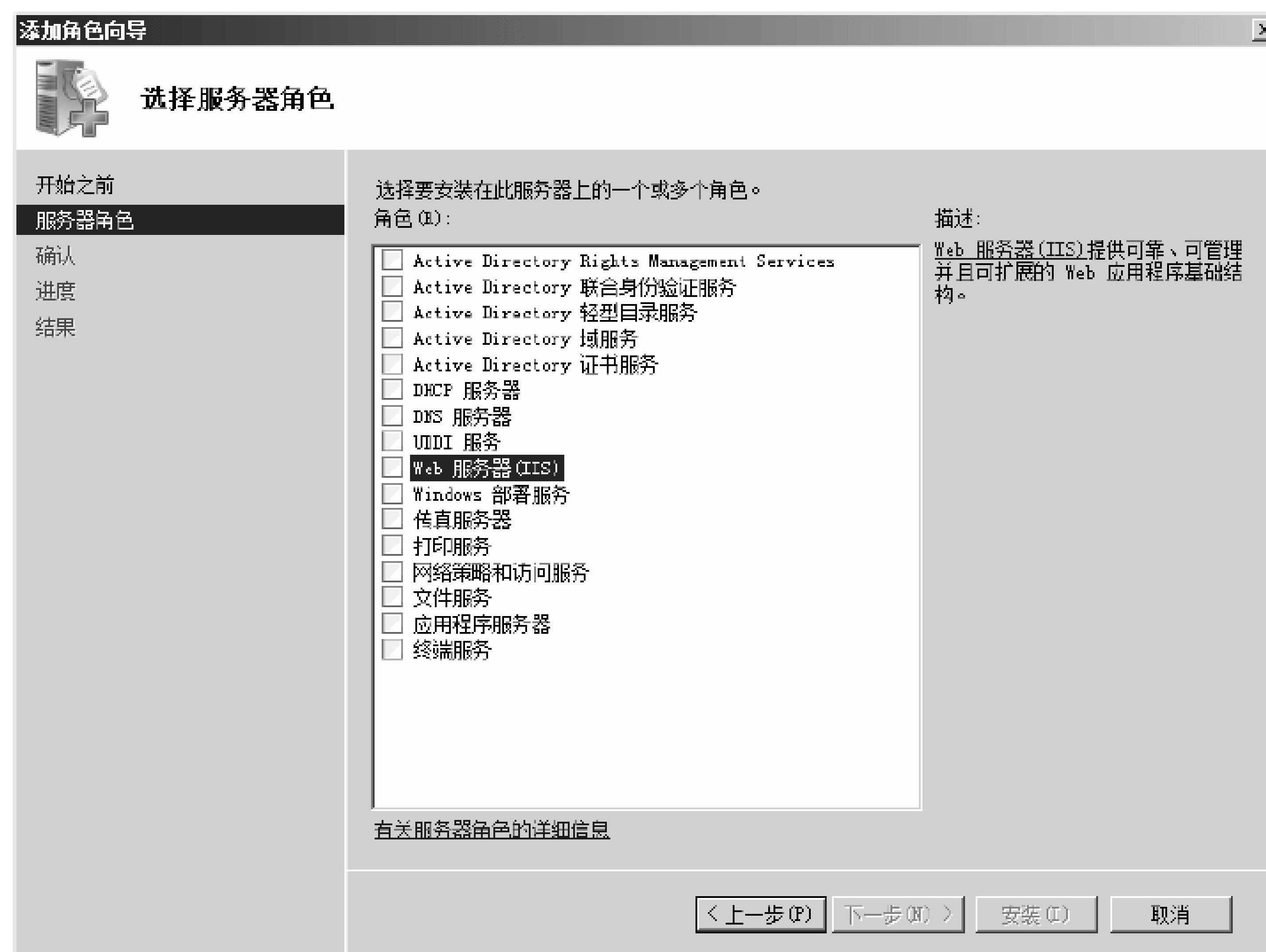


图 9-3 【添加服务器角色】对话框

04 弹出添加功能对话框，如图 9-4 所示，单击【添加必需的功能】按钮。

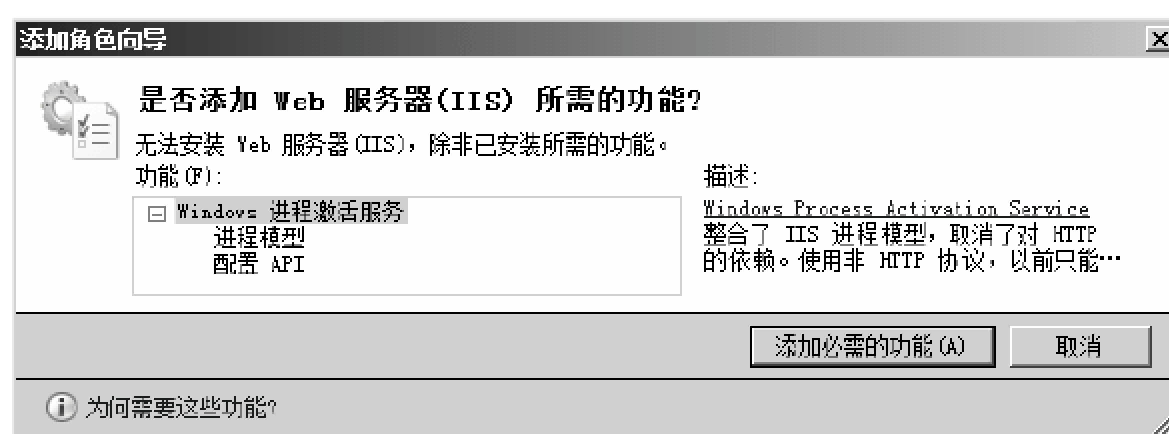


图 9-4　添加功能对话框

05 返回至【添加服务器角色】对话框，如图 9-5 所示，单击【下一步】按钮。

06 打开【Web 服务器】对话框，如图 9-6 所示，单击【下一步】按钮。



图 9-5 【添加服务器角色】对话框

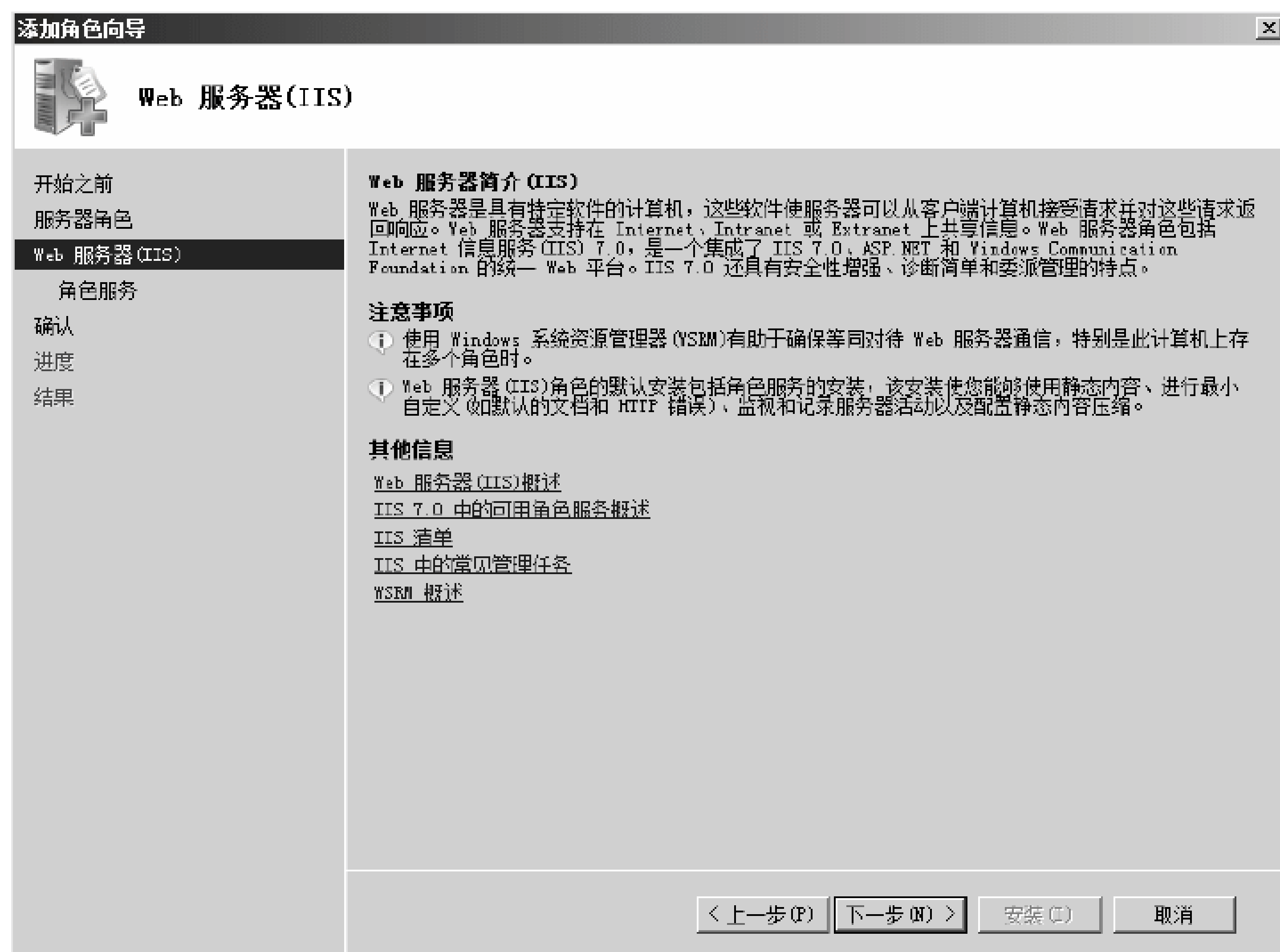


图 9-6 【Web 服务器】对话框

07 打开【选择角色服务】对话框，选择需要使用的 Web 服务器功能，本实例采用默认配置，以实现一般网站的发布，单击【下一步】按钮，如图 9-7 所示。

08 打开【确认安装选择】对话框，如图 9-8 所示，单击【安装】按钮。

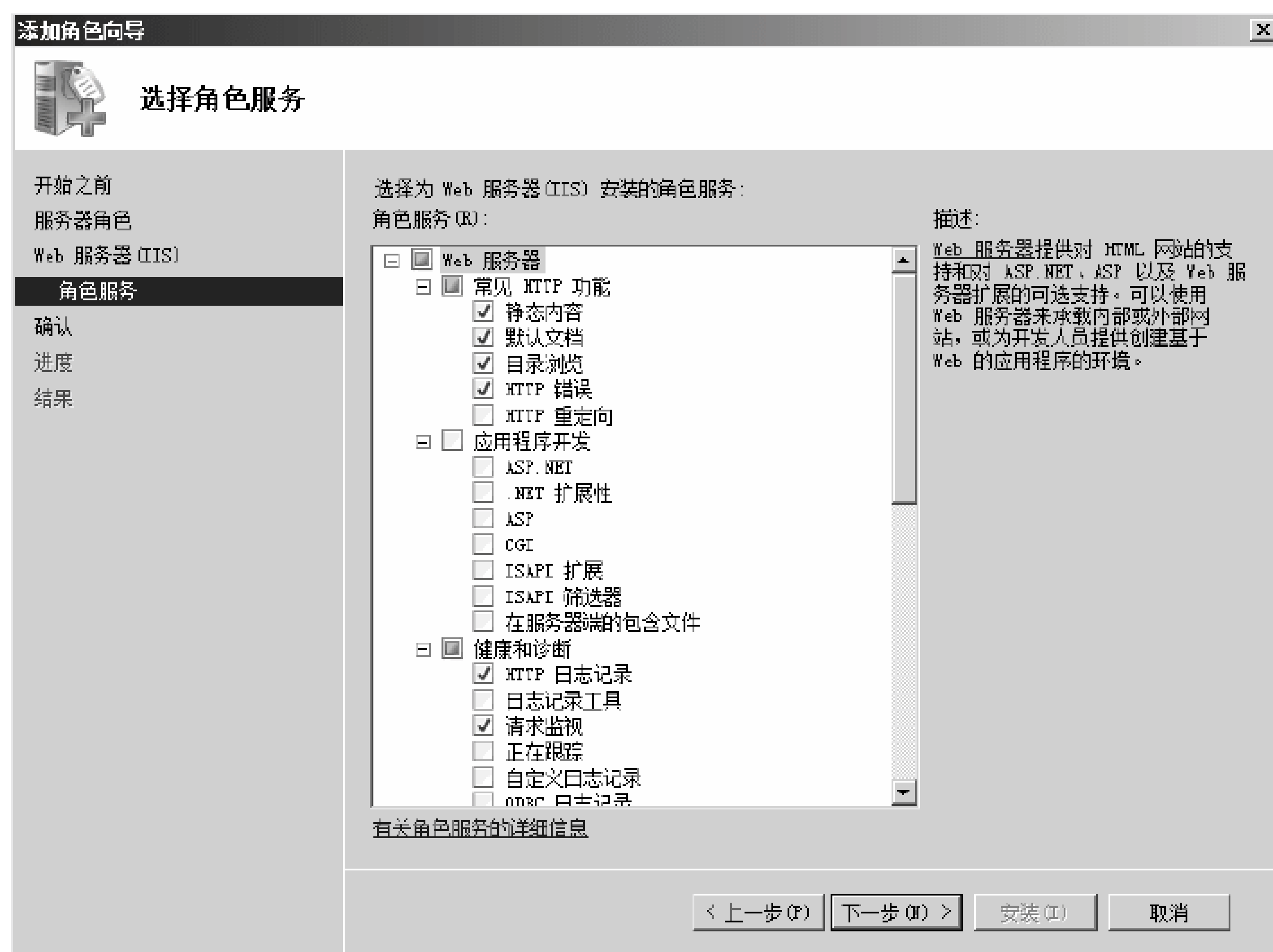


图 9-7 【选择角色服务】对话框



图 9-8 【确认安装选择】对话框

09 打开【安装进度】对话框，如图 9-9 所示，显示 Web 服务器安装进度。

10 打开【安装结果】对话框，提示安装成功，如图 9-10 所示，单击【关闭】按钮，完成 Web 服务器的安装。



图 9-9 【安装进度】对话框



图 9-10 【安装结果】对话框

9.2.2 发布网站

IIS 组件安装完成后，会建立一个默认站点，通过修改默认站点的相关属性可以在 Web 服务器上发布第一个网站。发布第一个网站的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，如图 9-11 所示。

02 弹出 Internet 信息服务管理器窗口，在左侧选项中右击 WIN-K3VD3TJ2RME (计算机名) ➢【网站】➢ Default Web Site 选项，在弹出的快捷菜单中选择【管理网站】➢【高级设置】命令，如图 9-12 所示。



图 9-11 【开始】选项菜单

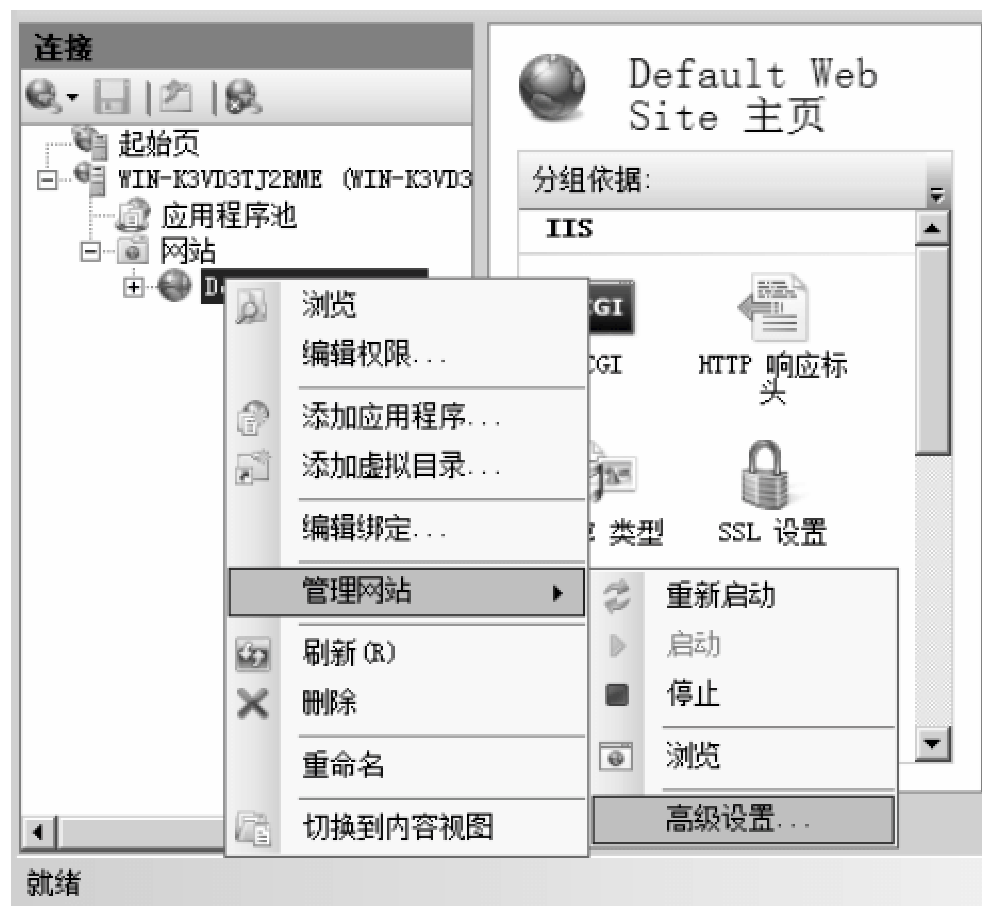


图 9-12 设置网站

03 弹出【高级设置】对话框，如图 9-13 所示，单击【物理路径】选项后面的...按钮。

04 弹出【浏览文件夹】对话框，浏览找到网站目录所在的物理路径。如图 9-14 所示，本实

例中网站目录物理路径为“C:\web ”，单击【确定】按钮。



图 9-13 【高级设置】对话框



图 9-14 【浏览文件夹】对话框

05 返回至 Internet 信息服务管理器窗口，如图 9-15 所示，双击【默认文档】图标。

06 打开【默认文档】窗格，如图 9-16 所示，单击选中【默认文档】窗格中的 Default.htm 名称，单击右侧【删除】按钮。



图 9-15 Internet 信息服务管理器窗口

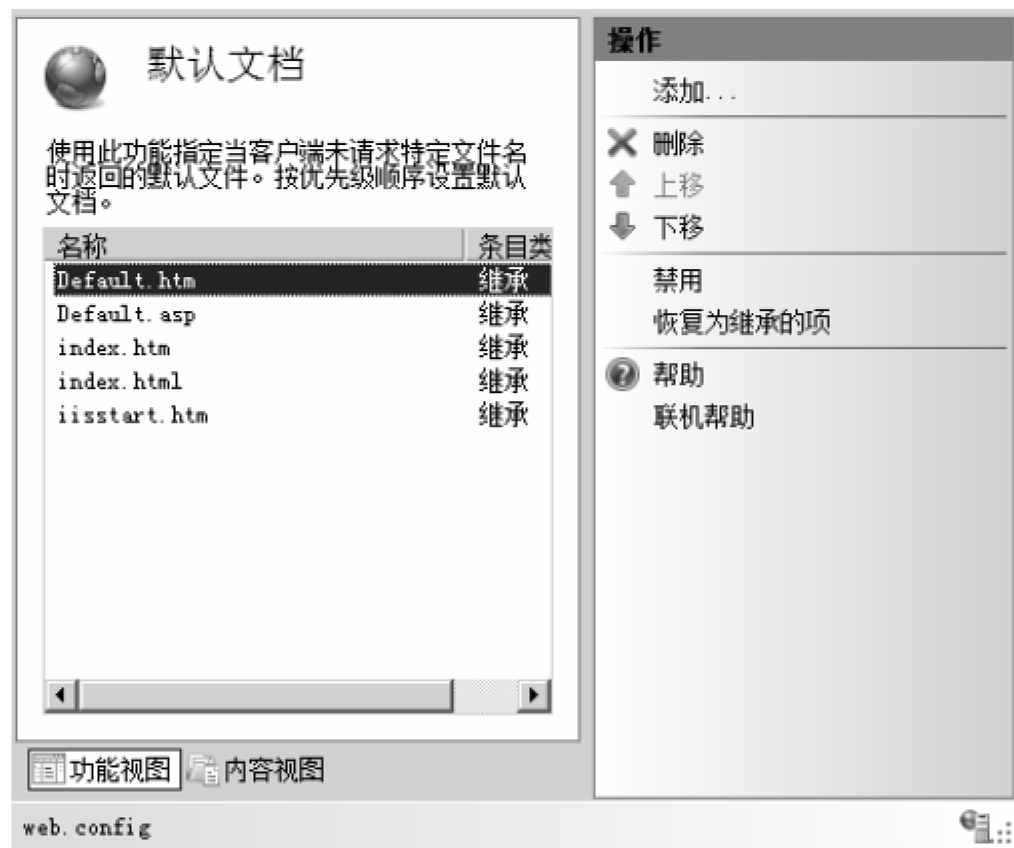


图 9-16 【默认文档】窗格

07 弹出【确认删除】提示框，如图 9-17 所示，单击【是】按钮。

08 依照上述步骤，如图 9-18 所示，依次将【默认文档】窗格中的所有默认名称删除。单击右侧【添加】链接。

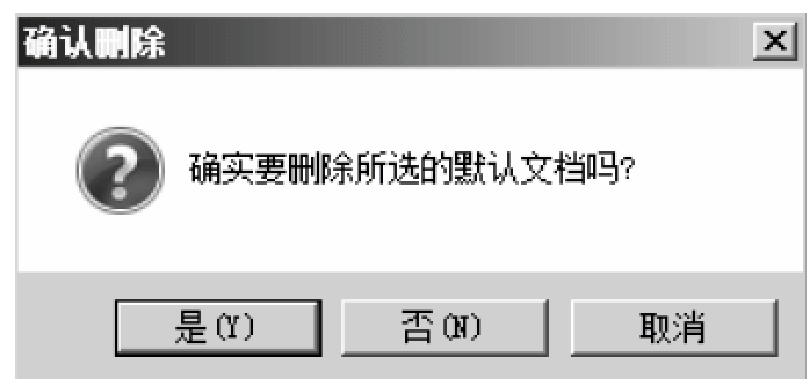


图 9-17　【确认删除】提示框

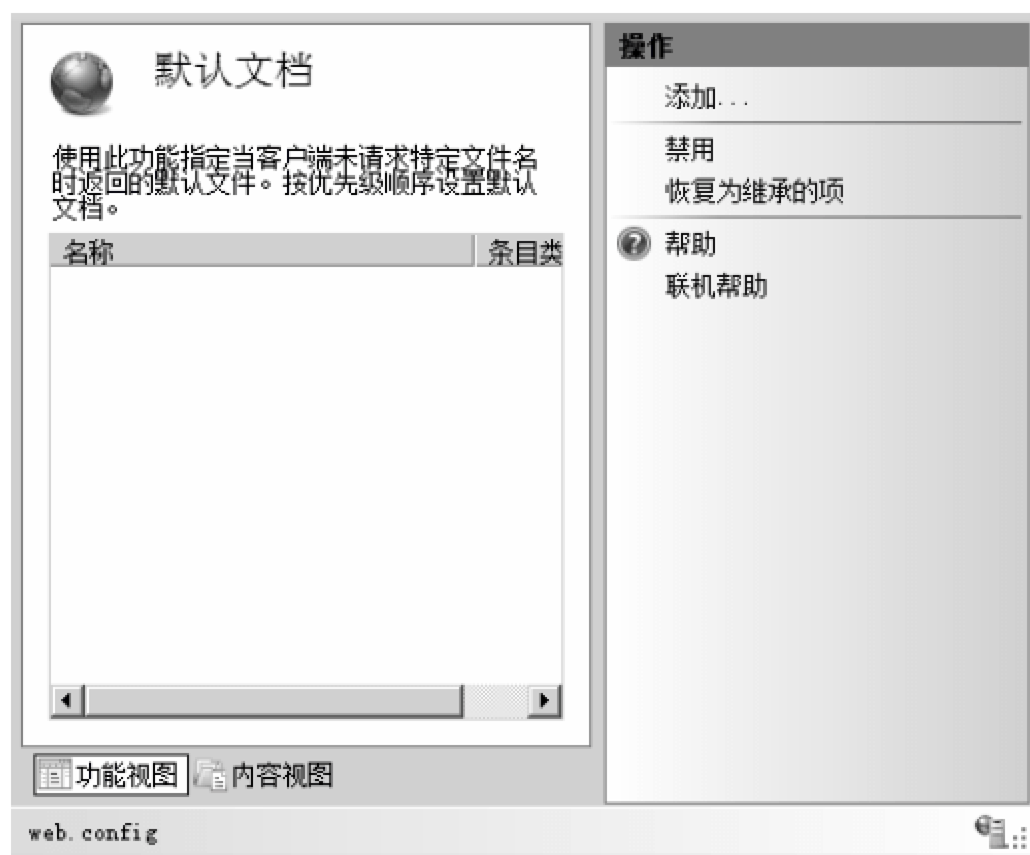


图 9-18　删除默认文档成功

09 弹出【添加默认文档】对话框，在【名称】文本框中输入网站主页文件的名称。本实例网站主页的名称为 index.html，如图 9-19 所示，单击【确定】按钮。

10 返回至 Internet 信息服务管理器窗口，如图 9-20 所示，IIS 发布网站结束。



图 9-19　【添加默认文档】对话框

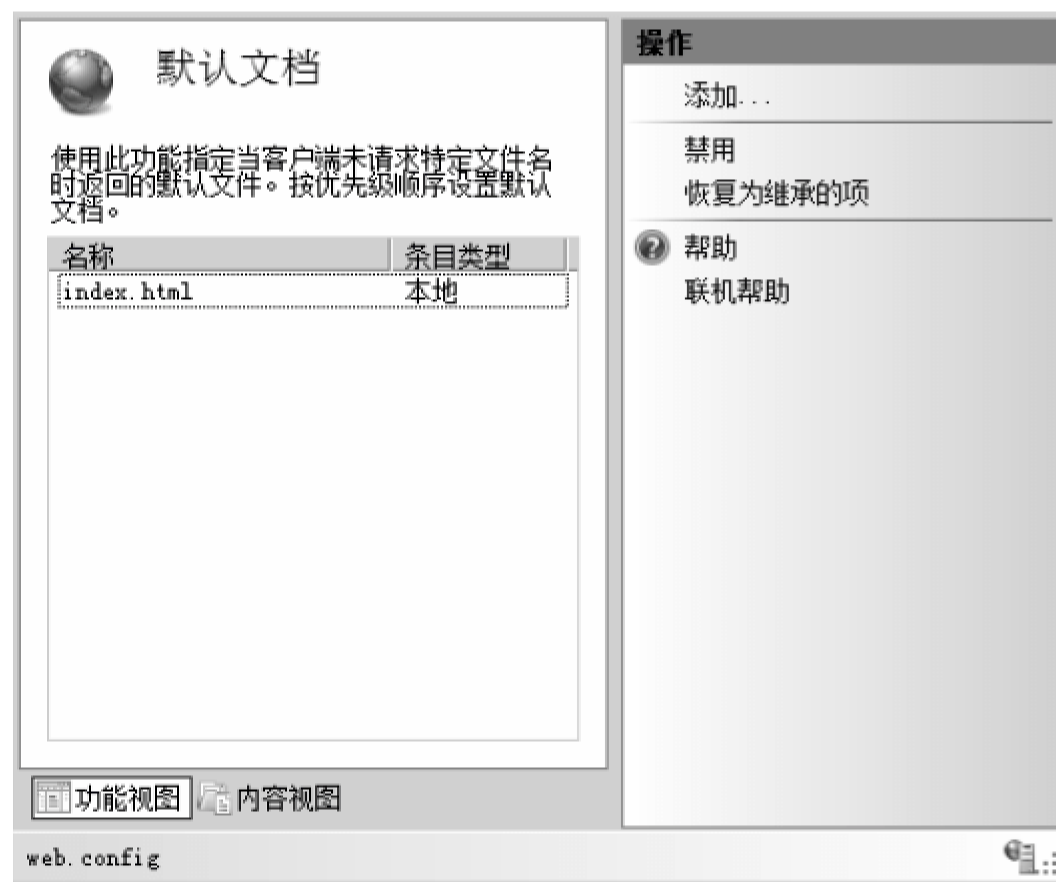


图 9-20　添加默认文档成功

11 客户端登录，如图 9-21 所示，打开 IE 浏览器，在地址栏里面输入“http: //192.168.1.200”，其中“192.168.1.200”为 Web 服务器的 IP 地址，按 Enter 键，成功访问到网站。



图 9-21　网站界面

9.3 使用 IIS 进行多网站发布

很多 Web 服务器都需要同时承担多个网站的发布工作，结合实际环境应当选用不同的方式实现多网站发布。发布多网站的方式可以总结为三种：区分 IP 发布多网站、区分端口发布多网站、区分主机头发布多网站。具体实现方法介绍如下。

9.3.1 使用不同的 IP 发布不同的网站

如果 Web 服务器有多个 IP 地址，则可以通过使用每个 IP 地址对应一个网站来使用一个服务器发布多个网站。下面建立 www.jianfeng.com 和 mail.jianfeng.com 两个网站，每个网站分别对应一个 IP 地址，具体的 IP 规划如表 9-1 所示。

表 9-1

域名	IP 地址	主目录物理路径	默认文档
www.jianfeng.com	192.168.1.200	C:\Web 1	index.html
mail.jianfeng.com	192.168.1.201	C:\Web 2	index.html

将网站域名注册到 DNS，如图 9-22 所示。

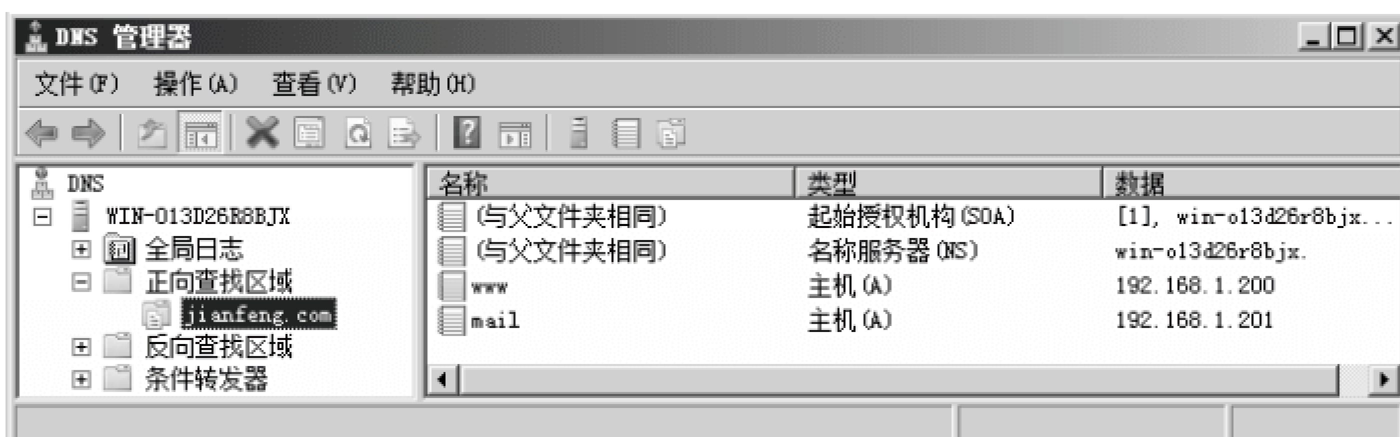


图 9-22　域名注册窗口

使用不同的 IP 发布不同的网站具体的操作步骤如下。

01 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项。

02 弹出 Internet 信息服务管理器窗口，在左侧选项中右击 WIN-013D26R8BJX ➢【网站】➢【Default Web Site】选项，在弹出的快捷菜单中选择【删除】命令，如图 9-23 所示。

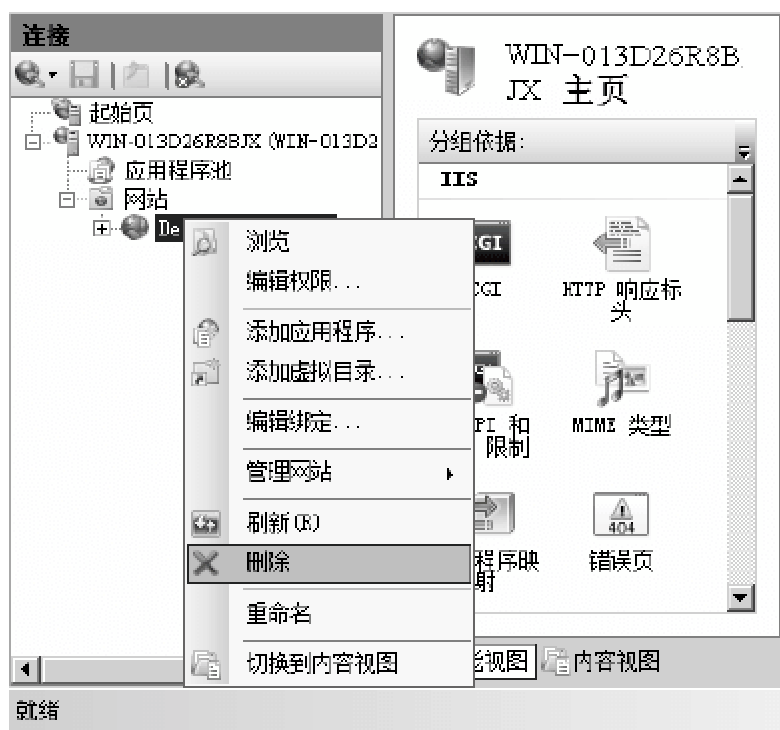


图 9-23　删除网站

03 弹出【确认删除】提示框，如图 9-24 所示，单击【是】按钮。

04 返回至 Internet 信息服务管理器对话框，如图 9-25 所示，右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

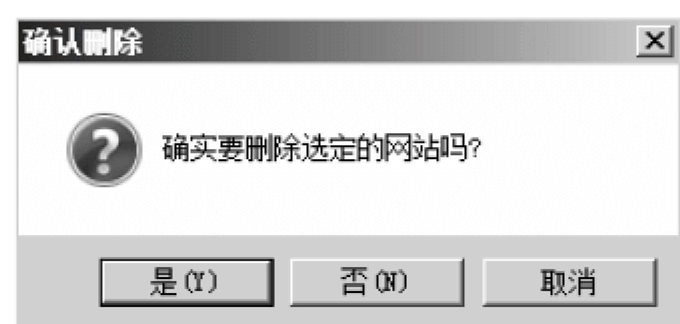


图 9-24 【确认删除】提示框



图 9-25 添加网站

05 弹出【添加网站】对话框，在【网站名称】文本框中输入网站名称，本实例网站名称为“web 1”，单击【物理路径】文本框后面的 .. 按钮，如图 9-26 所示。

06 弹出【浏览文件夹】对话框，浏览找到网站目录的物理路径，本实例为“C:/web 1”，单击【确定】按钮，如图 9-27 所示。

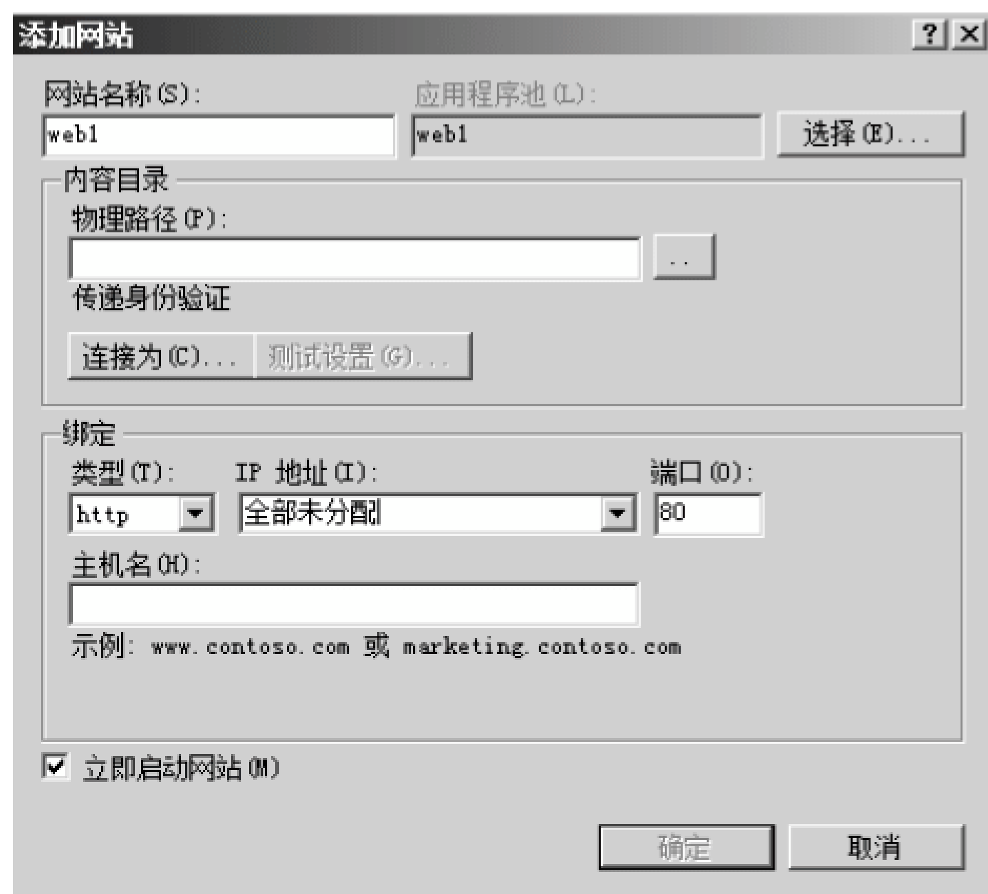


图 9-26 【添加网站】对话框

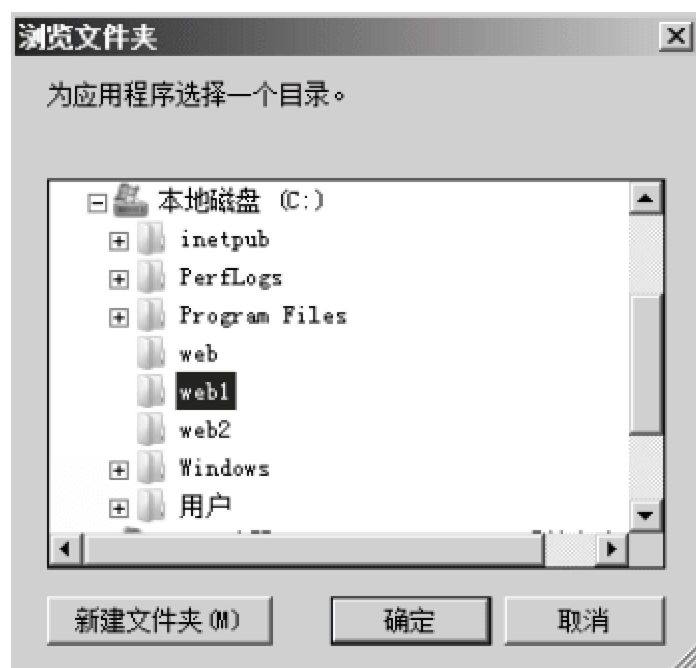


图 9-27 【浏览文件夹】对话框

07 返回至【添加网站】对话框，在【IP 地址】下拉列表框中选择 IP 地址为“192.168.1.200”，在【主机名】文本框中输入该网站的域名，如图 9-28 所示，本实例为 www.jianfeng.com，选中【立即启动网站】复选框，单击【确定】按钮。

08 返回至 Internet 信息服务管理器窗口，选择左侧【web 1】选项，如图 9-29 所示，双击【web 1 主页】窗格下面的【默认文档】图标。

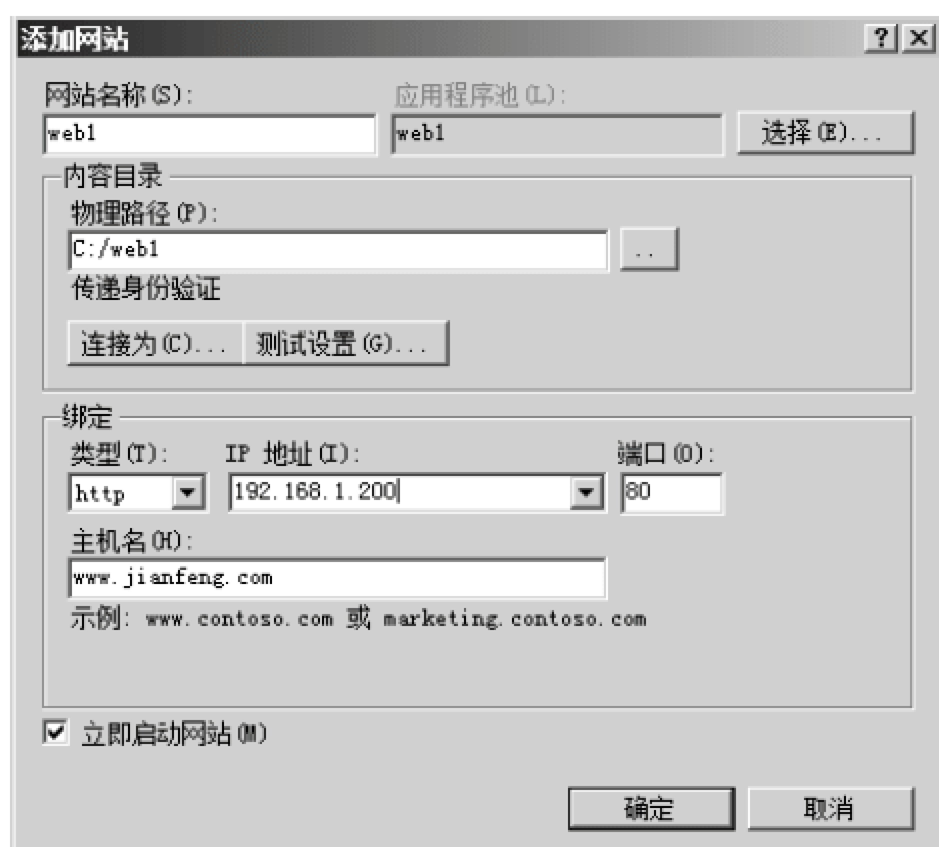


图 9-28 【添加网站】对话框



图 9-29 新站点添加成功

09 打开【默认文档】对话框，选择【默认文档】窗格中的【Default.htm】选项，单击右侧【删除】链接。

10 弹出【确认删除】提示框，单击【是】按钮。

11 返回至 Internet 信息服务管理器窗口，依照上述步骤删除【默认文档】窗格中所有内容，单击右侧【添加】链接。

12 弹出【添加默认文档】对话框，在【名称】文本框中输入该网站的主页名称，本实例输入默认文档名为 index.html，单击【确定】按钮。

13 返回至 Internet 信息服务管理器窗口，如图 9-30 所示，右击左侧【Web 1】选项，在弹出的快捷菜单中单击【管理网站】➢【浏览】命令。

14 打开域名为“www.jianfeng.com”的网站，如图 9-31 所示，表示第一个网站发布成功。



图 9-30 Internet 信息服务管理器窗口



图 9-31 尖峰网站

15 发布第二个网站。选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，弹出 Internet 信息服务管理器窗口，选中 WIN-013D26R8BJX 选项，右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

16 弹出【添加网站】对话框，在【网站名称】文本框中输入网站的名称，如图 9-32 所示，

本实例输入“web 2”，单击【物理路径】文本框后面的..按钮。

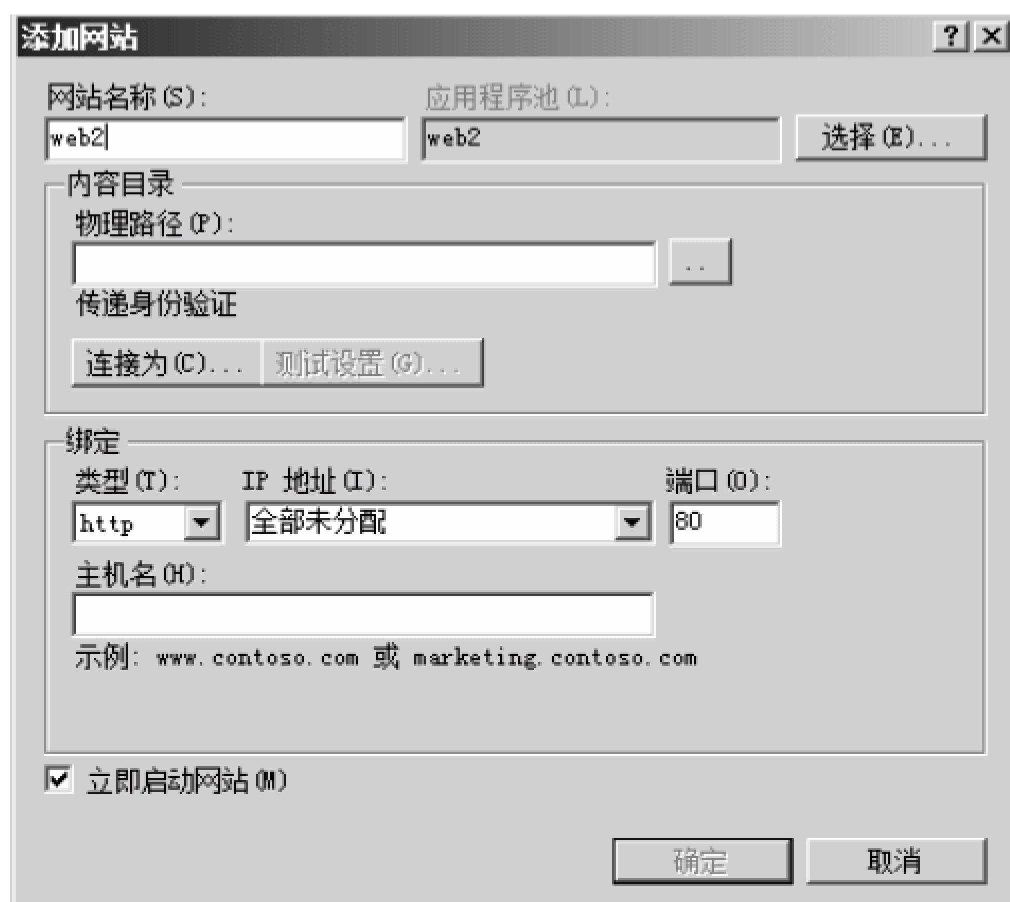


图 9-32　设置网站名称

17 弹出【浏览文件夹】对话框，浏览找到网站 web 2 的物理路径，如图 9-33 所示，本实例为“C:/web 2”，单击【确定】按钮。

18 返回至【添加网站】对话框，如图 9-34 所示，在【IP 地址】下拉列表框中选择“192.168.1.201”，在【主机名】文本框中输入网站 web 2 的域名，本实例为“mail.jianfeng.com”，单击【确定】按钮。



图 9-33　【浏览文件夹】对话框

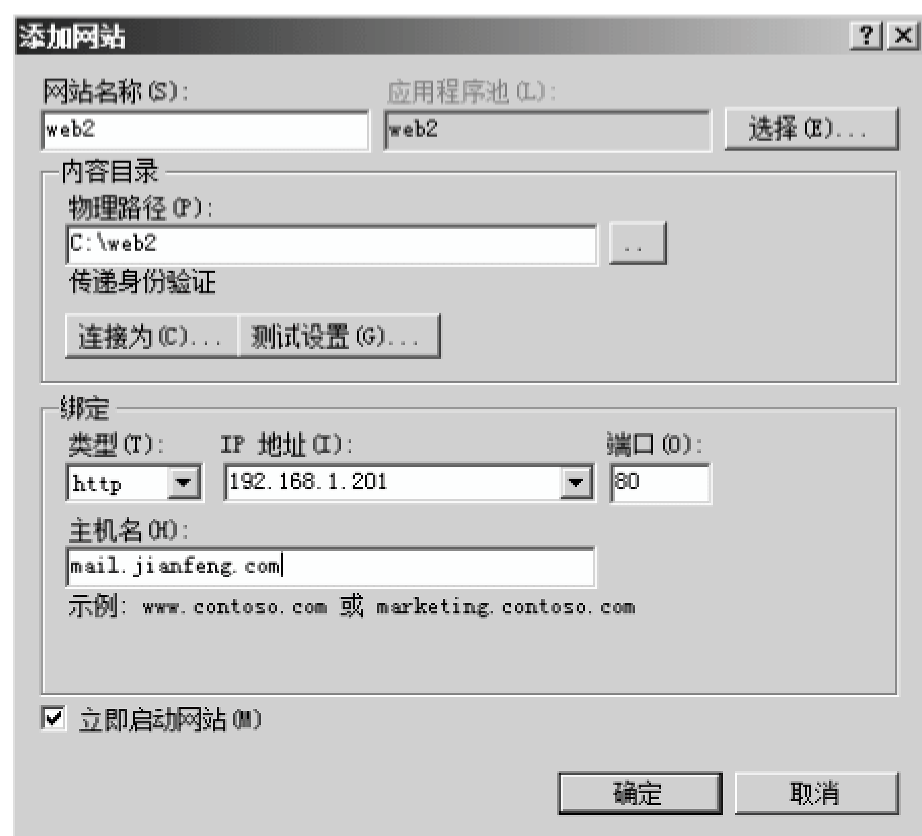


图 9-34　设置 IP 地址和主机名

19 返回至 Internet 信息服务管理器窗口，选择【web 2】选项，在【web 2 主页】窗格下方双击【默认文档】图标，如图 9-35 所示。

20 打开【默认文档】窗格，选择 Default.htm 选项，单击右侧【删除】按钮。



图 9-35　【web2 主页】窗格

21 弹出【确认删除】提示框，单击【是】按钮。

22 返回至【默认文档】窗格，单击右侧【添加】链接。

23 弹出【添加默认文档】对话框，在【名称】文本框中输入网站 web 2 的主页名称，本实例为 index.html，单击【确定】按钮。

24 返回至 Internet 信息服务管理器窗口，如图 9-36 所示，右击选中 web 2 选项，在弹出的快捷菜单中选择【管理网站】➢【浏览】命令。



图 9-36　【Internet 信息服务（IIS）管理器】窗口

25 打开域名为 mail.jianfeng.com 的网站，如图 9-37 所示，至此第二网站发布成功。



图 9-37　尖峰网站界面

9.3.2 使用同一 IP 地址不同的端口发布不同的网站

如果 Web 服务器只有一个 IP 地址，则可以使用同一 IP 地址的不同端口来发布不同的网站，从而实现一个服务器发布多个网站。下面建立 www.jianfeng.com 和 mail.jianfeng.com 两个网站，两个网站使用同一 IP 地址不同的端口进行访问，具体的 IP 和端口规划如表 9-2 所示。

表 9-2 IP 和端口规划

域名	IP 地址	主目录物理路径	默认文档	端口
www.jianfeng.com	192.168.1.200	C:/web 1	index.html	80
mail.jianfeng.com	192.168.1.200	C:/web 2	index.html	8080

使用同一 IP 地址不同的端口发布不同的网站的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，弹出 Internet 信息服务管理器窗口，如图 9-38 所示，选中 WIN-013D26R8BJX 选项，右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

02 弹出【添加网站】对话框，在【网站名称】文本框中输入网站的名称，本实例为“web 1”，单击【物理路径】文本框后面的 ... 按钮。

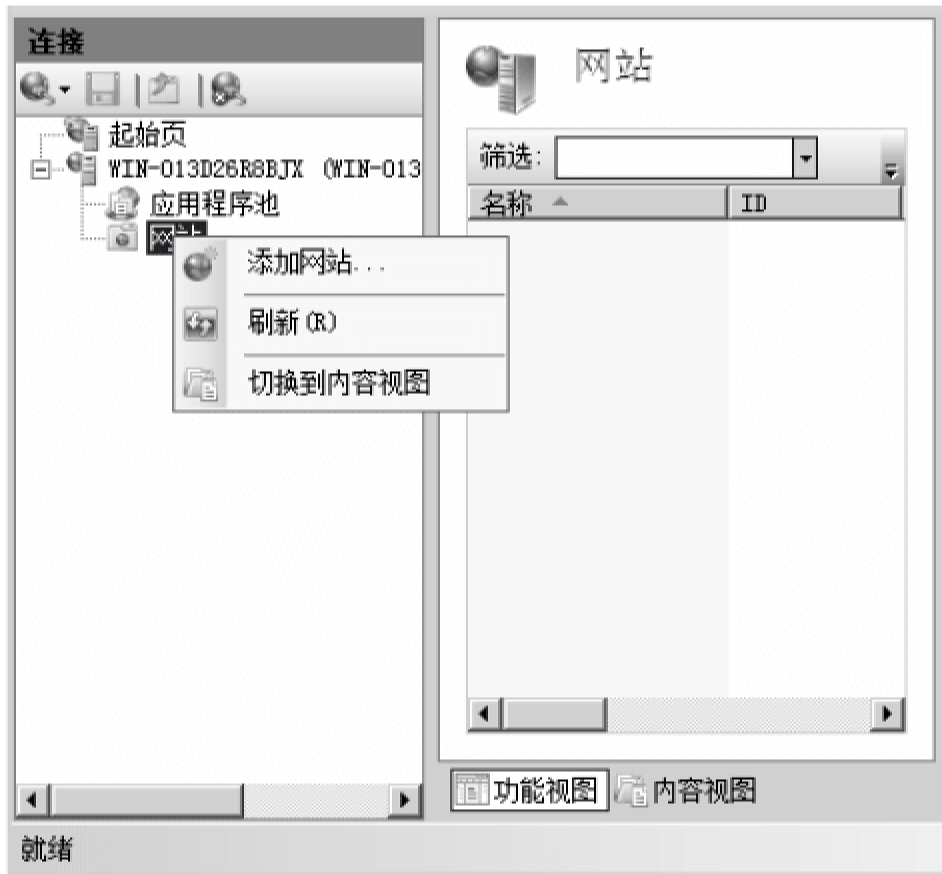


图 9-38 添加新网站

03 弹出【浏览文件夹】对话框，找到网站 Web 1 的主目录的物理路径，本实例为“C:/web 1”，单击【确定】按钮。

04 返回至【添加网站】对话框，在【IP 地址】下拉列表框中选择 IP 地址为“192.168.1.200”，在【端口】文本框中输入端口号为“80”，单击【确定】按钮。

05 返回至 Internet 信息服务管理器窗口，选择左侧 web 1 选项，双击【web 1 主页】窗格中的【默认文档】图标。

06 打开【默认文档】窗格，选择 Default.htm 选项，单击右侧【删除】按钮。

07 弹出【确认删除】提示框，单击【是】按钮。

08 返回至 Internet 信息服务管理器窗口，依照上述步骤删除【默认文档】窗格中所有内容，单击右侧【添加】链接。

09 弹出【添加默认文档】对话框，在【名称】文本框中输入该网站的主页名称，本实例输入为 index.html，单击【确定】按钮。

10 返回至 Internet 信息服务管理器窗口，至此网站 web 1 发布完成。右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

11 弹出【添加网站】对话框，单击【物理路径】文本框后面的 .. 按钮。

12 弹出【浏览文件夹】对话框，浏览找到网站 web 2 的物理路径，本实例为"C：/web 2"，单击【确定】按钮。

13 返回至【添加网站】对话框，在【IP 地址】下拉列表框中选择 IP 地址为"192.168.1.200"，在【端口】文本框中输入端口号为"8080"，单击【确定】按钮。

14 返回至 Internet 信息服务管理器窗口，选择左侧 web 2 选项，双击【web 2 主页】窗格中的【默认文档】图标。

15 打开【默认文档】窗格，选择【默认文档】窗格中的 Default.htm 选项，单击右侧【删除】按钮，如图 9-39 所示。

16 弹出【确认删除】提示框，单击【是】按钮，如图 9-40 所示。



图 9-39 【默认文档】窗格

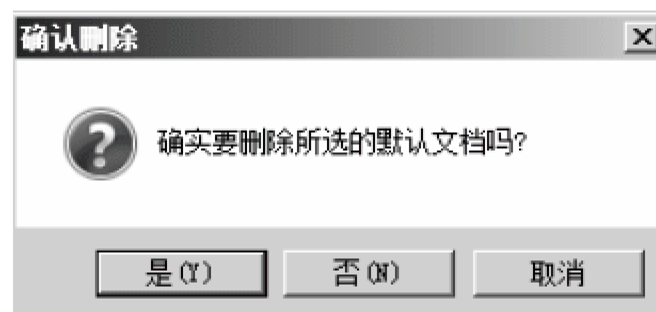


图 9-40 【确认删除】提示框

17 返回至【默认文档】窗格，依照上述步骤将【默认文档】窗格中的所有默认文档删除，单击右侧【添加】链接。

18 弹出【添加默认文档】对话框，在【名称】文本框中输入网站 web 2 的主页名称，本实例为 index.html，单击【确定】按钮，如图 9-41 所示。



图 9-41 【添加默认文档】对话框

19 返回至 Internet 信息服务管理器窗口，至此网站 web 2 创建完成。

20 客户端访问。打开 IE 浏览器，在地址栏输入"http://192.168.1.200: 80"，其中"192.168.1.200"

为 Web 服务器的 IP 地址，80 为访问网站使用的 HTTP 协议的端口号，按 Enter 键，如图 9-42 所示，可以正常打开网站 web 1。



图 9-42　80 端口访问网站

21 客户端访问。打开 IE 浏览器，在地址栏输入“http://192.168.1.200: 8080”，其中“192.168.1.200”为 Web 服务器的 IP 地址，8080 为访问网站使用的 HTTP 协议的端口号，按 Enter 键，如图 9-43 所示，可以正常打开网站 web 2。



图 9-43　8080 端口访问网站

9.3.3　利用不同主机头发布不同的网站

如果 Web 服务器只有一个 IP 地址，则可以使用不同的主机头来发布不同的网站，从而实现一个服务器发布多个网站。下面建立 www.jianfeng.com 和 mail.jianfeng.com 两个网站，两个网站使用同一 IP 地址不同的主机头进行访问，具体的 IP 和主机头规划如表 9-3 所示。

表 9-3　IP 和主机头规划

域名（主机头）	IP 地址	主目录物理路径	默认文档	端口
www.jianfeng.com	192.168.1.200	C:\web 1	index.html	80
mail.jianfeng.com	192.168.1.200	C:\web 2	index.html	80

将网站域名注册到 DNS，如图 9-44 所示。

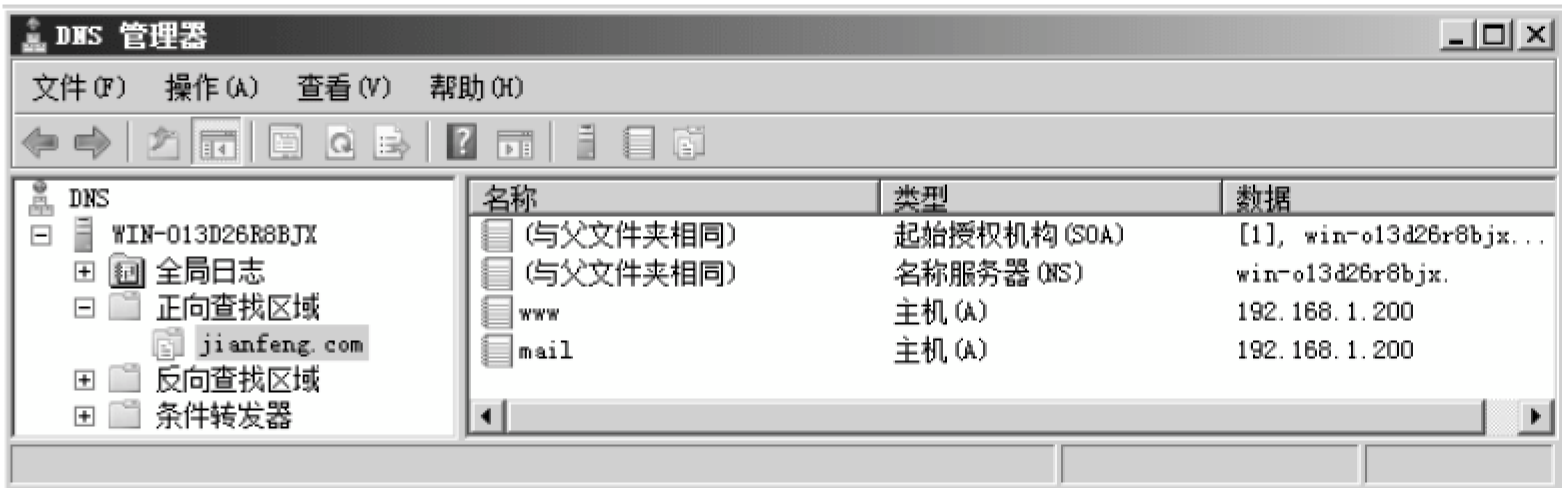


图 9-44　域名注册界面

利用不同主机头发布不同网站的具体操作步骤如下：

01 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】命令，弹出 Internet 信息服务管理器窗口，选择 WIN-013D26R8BJX，右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

02 弹出【添加网站】对话框，在【网站名称】文本框中输入网站的名称，本实例为 web 1，单击【物理路径】文本框后面的 .. 按钮。

03 弹出【浏览文件夹】对话框，找到网站 web 1 的主目录的物理路径，本实例为“C:\web 1”，单击【确定】按钮。

04 返回至【添加网站】对话框，在【IP 地址】下拉列表框中选择 IP 地址为“192.168.1.200”，在【端口号】文本框中输入 80，在【主机名】文本框中输入网站 web 1 的域名，本实例为“www.jianfeng.com”，单击【确定】按钮。

05 返回至 Internet 信息服务管理器窗口，选择左侧 web 1 选项，双击【web 1 主页】窗格的【默认文档】图标。

06 打开【默认文档】窗格，选择【默认文档】窗格中的 Default.htm 选项，单击右侧【删除】按钮。

07 弹出【确认删除】提示框，单击【是】按钮。

08 返回至 Internet 信息服务管理器窗口，依照上述步骤删除【默认文档】窗格中所有默认文档，单击右侧【添加】链接。

09 弹出【添加默认文档】对话框，在【名称】文本框中输入该网站的主页名称，本实例为“index.html”，单击【确定】按钮。

10 返回至 Internet 信息服务管理器窗口，至此网站 web 1 发布完成。右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

11 弹出【添加网站】对话框，在【网站名称】文本框中输入网站 web 2 的网站名称，本实例为 web 2，单击【物理路径】文本框后面的 .. 图标。

12 弹出【浏览文件夹】对话框，找到网站 web 2 的物理路径，本实例为“C:\web 2”，单击【确定】按钮。

13 返回至【添加网站】对话框，在【IP 地址】下拉列表框中选择 IP 地址为“192.168.1.200”，在【主机名】文本框中输入网站 web 2 的域名，本实例为“mail.jianfeng.com”，单击【确定】按钮。

14 返回至 Internet 信息服务管理器窗口，选中左侧 web 2 选项，双击【web 2 主页】窗格中的【默认文档】图标。

15 打开【默认文档】窗格，选择 Default.htm 选项，单击右侧【删除】按钮。

16 弹出【确认删除】提示框，单击【是】按钮。

17 返回至【默认文档】窗格，依照上述步骤将【默认文档】窗格中的所有默认文档删除，单击右侧【添加】链接。

18 弹出【添加默认文档】对话框，在【名称】文本框中输入网站 web 2 的主页名称，本实例为 index.html，单击【确定】按钮。

19 返回至 Internet 信息服务管理器窗口，至此网站 web 2 创建完成。

20 客户端访问测试，如图 9-45 所示，打开 IE 浏览器，在地址栏里面输入 http://www.jianfeng.com，其中 wwww.jianfeng.com 为网站 web 1 的域名，按 Enter 键，可以正确地打开网站 web 1。



图 9-45　网站 web 1 截图

21 客户端访问测试，如图 9-46 所示，打开 IE 浏览器，在地址栏里面输入 http://mail.jianfeng.com，按 Enter 键，可以打开网站 web 2。



图 9-46　网站 web 2 截图

9.4　项目实战 2：使用 SSL 确保 Web 服务器通信安全

当在网站上进行数据上传和下载的时候，这些数据就有可能被互联网用户获取，从而导致数据泄露。SSL（secure socket layer）是一个以 PKI 为基础的安全协议，若要让网站拥有 SSL 安全连接功能，就必须为网站向证书颁发机构（CA）申请 SSL 证书，证书中包含了公钥、证书有效期限、发放此证书的 CA、CA 的数据签名等数据，当网站有了 SSL 证书之后，客户端与网站之间就可以通过 SSL 安全连接来进行通信，如果有非法用户窃取数据，数据将会以加密形式存在，从而保证数据的安全性。

客户端在访问拥有 SSL 安全证书的网站的时候，应该将网址中的“http”改为“https”，如网站“mail.jianfeng.com”拥有并启用了 SSL 安全证书，在访问的时候使用网址为“https://mail.jianfeng.com”。

下面详细介绍使用 SSL 确保 Web 服务器通信安全的详细步骤。

9.4.1　建立 CA 服务器

网站首先需要向证书颁发机构 CA 进行证书申请，如果是对外开放的商业网站，最好向知名的 CA 机构进行申请；如果是内部网络使用，则可以使用 Windows Server 2008 系统建立自己的 CA 机构。使用 Windows Server 2008 建立独立根 CA 的具体操作步骤如下。

01 右击【计算机】图标，如图 9-47 所示，在弹出的快捷菜单中选择【管理】命令。

02 打开【服务器管理器】窗口，选择左侧【角色】选项，如图 9-48 所示，单击右侧【添加角色】链接。





图 9-47 【计算机】快捷菜单　　　　图 9-48 【服务器管理器】窗口

03 弹出【开始之前】对话框，单击【下一步】按钮。

04 打开【选择服务器角色】对话框，如图 9-49 所示，选中【Active Directory 证书服务】复选框，单击【下一步】按钮。



图 9-49 【选择服务器角色】对话框

05 打开【Active Directory 证书服务简介】对话框，如图 9-50 所示，单击【下一步】按钮。

06 打开【选择角色服务】对话框，如图 9-51 所示，选中【证书颁发机构 Web 注册】复选框。

07 弹出【添加角色向导】对话框，如图 9-52 所示，单击【添加必需的角色服务】按钮。

08 返回至【添加角色向导】对话框，如图 9-53 所示，选中【联机响应程序】复选框，单击【下一步】按钮。



图 9-50 【Active Directory 证书服务简介】对话框

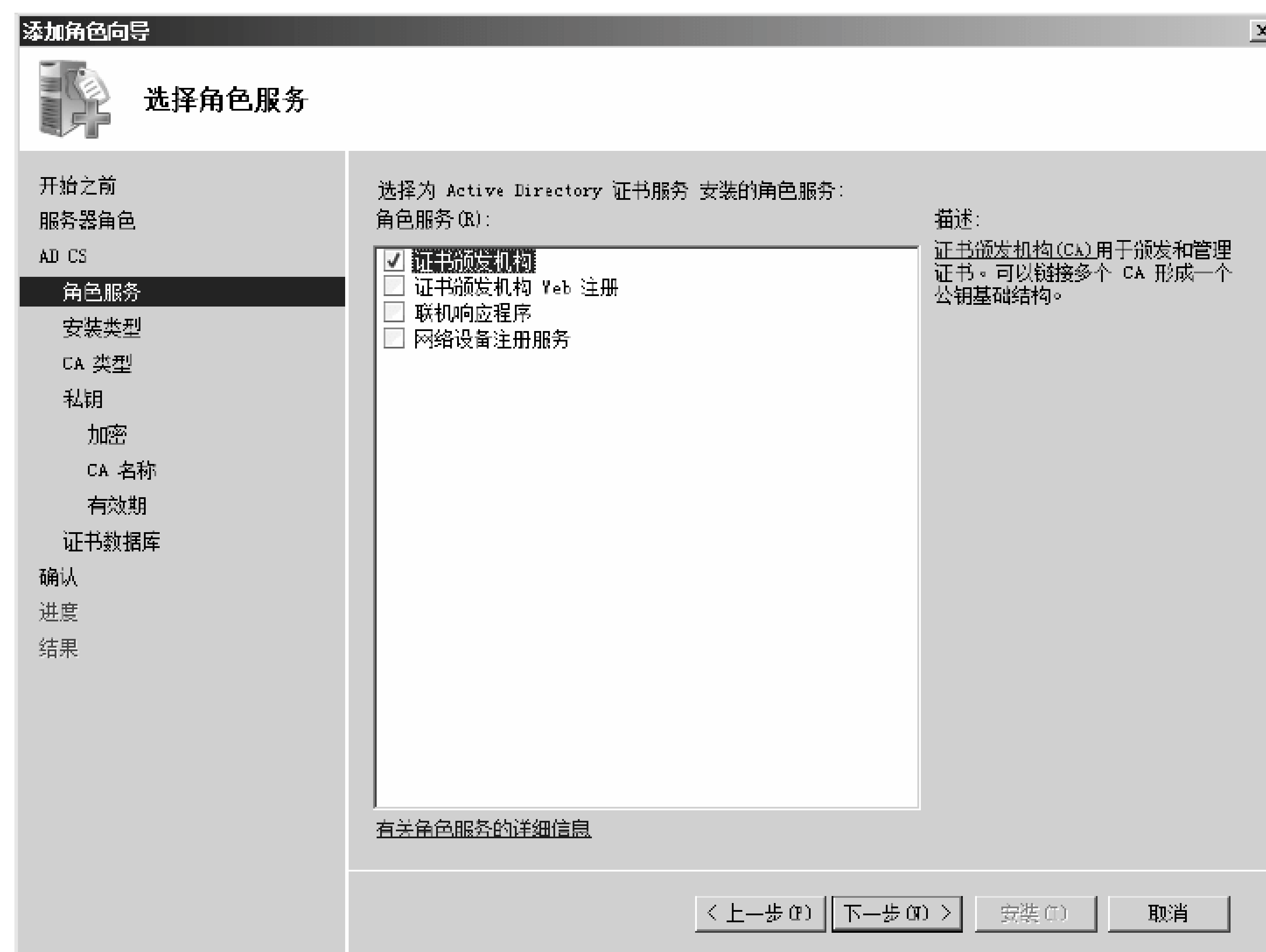


图 9-51 【选择角色服务】对话框 1

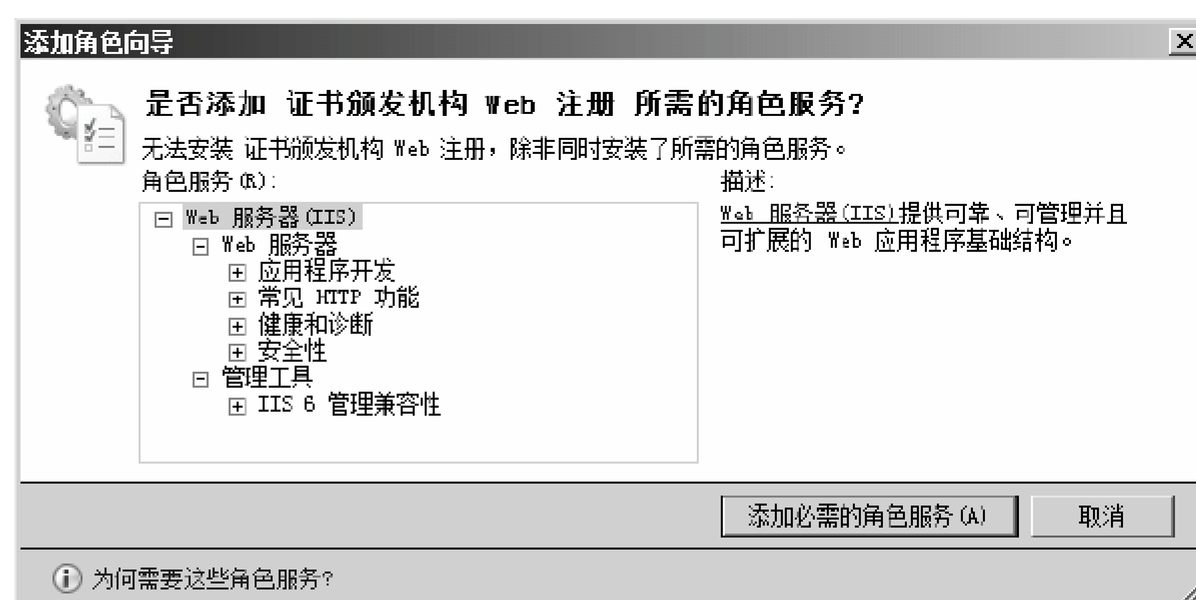


图 9-52 添加角色服务提示框



图 9-53　【选择角色服务】对话框 2

09 打开【指定安装类型】对话框，如图 9-54 所示，选中【独立】单选按钮，单击【下一步】按钮。

10 打开【指定 CA 类型】对话框，如图 9-55 所示，选中【根 CA】单选按钮，单击【下一步】按钮。



图 9-54　【指定安装类型】对话框



图 9-55 【指定 CA 类型】对话框

11 打开【设置私钥】对话框；选择【新建私钥】单选按钮，如图 9-56 所示，单击【下一步】按钮。

12 打开【为 CA 配置加密】对话框，如图 9-57 所示，单击【下一步】按钮。



图 9-56 【设置私钥】对话框



图 9-57 【为 CA 配置加密】对话框

13 打开【配置 CA 名称】对话框，在【此 CA 的公用名称】文本框中输入 CA 的公用名称，如图 9-58 所示，本实例为 tiankong，单击【下一步】按钮。

14 打开【设置有效期】对话框，如图 9-59 所示，单击【下一步】按钮。



图 9-58 【配置 CA 名称】对话框



图 9-59 【设置有效期】对话框

15 打开【配置证书数据库】对话框，如图 9-60 所示，单击【下一步】按钮。

16 弹出【Web 服务器（IIS）】对话框，如图 9-61 所示，单击【下一步】按钮。



图 9-60 【配置证书数据库】对话框

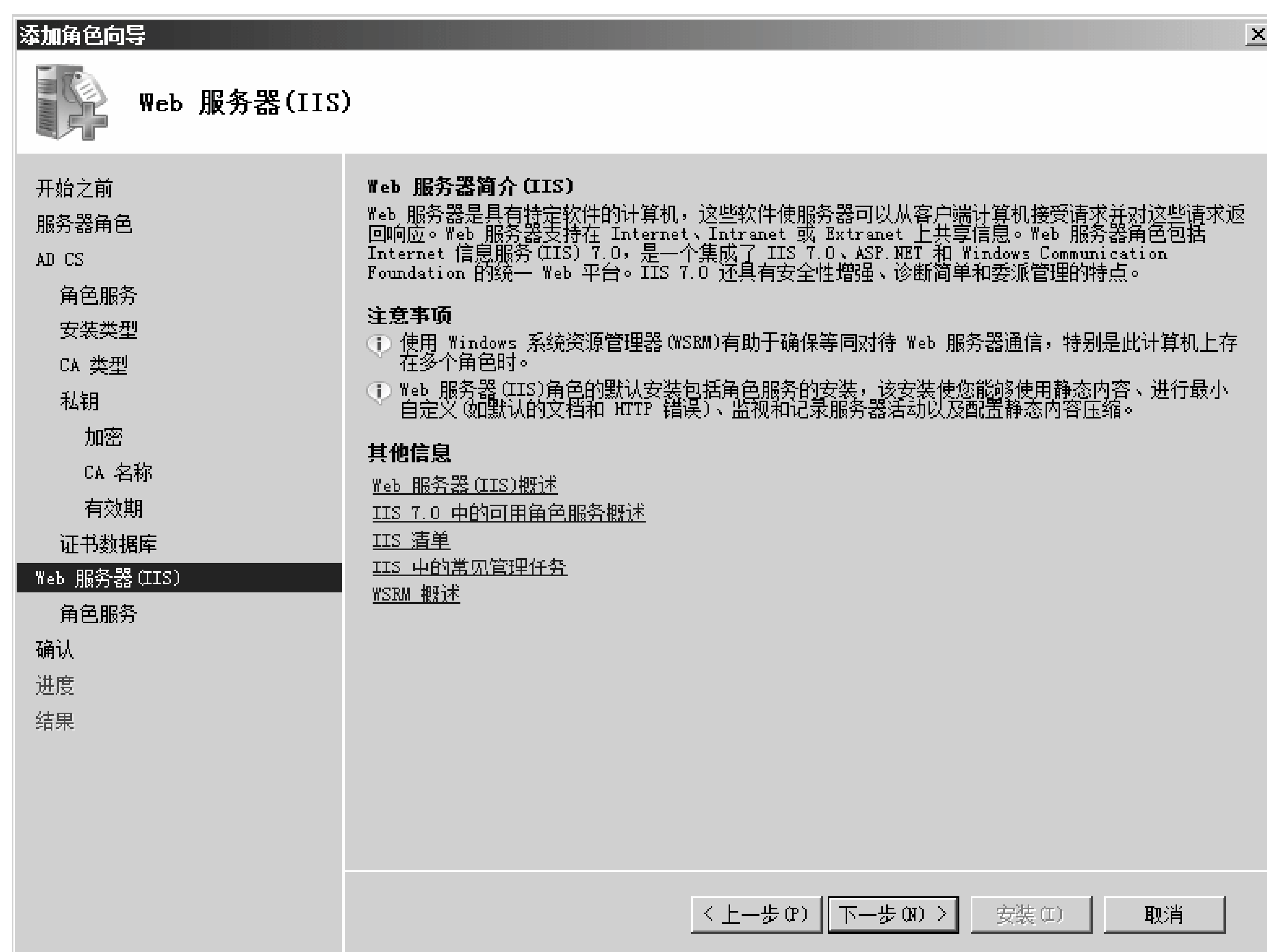


图 9-61　【Web 服务器（IIS）】对话框

17 打开【选择角色服务】对话框，如图 9-62 所示，单击【下一步】按钮。

18 打开【确认安装选择】对话框，确认安装信息无误时，如图 9-63 所示，单击【安装】按钮。

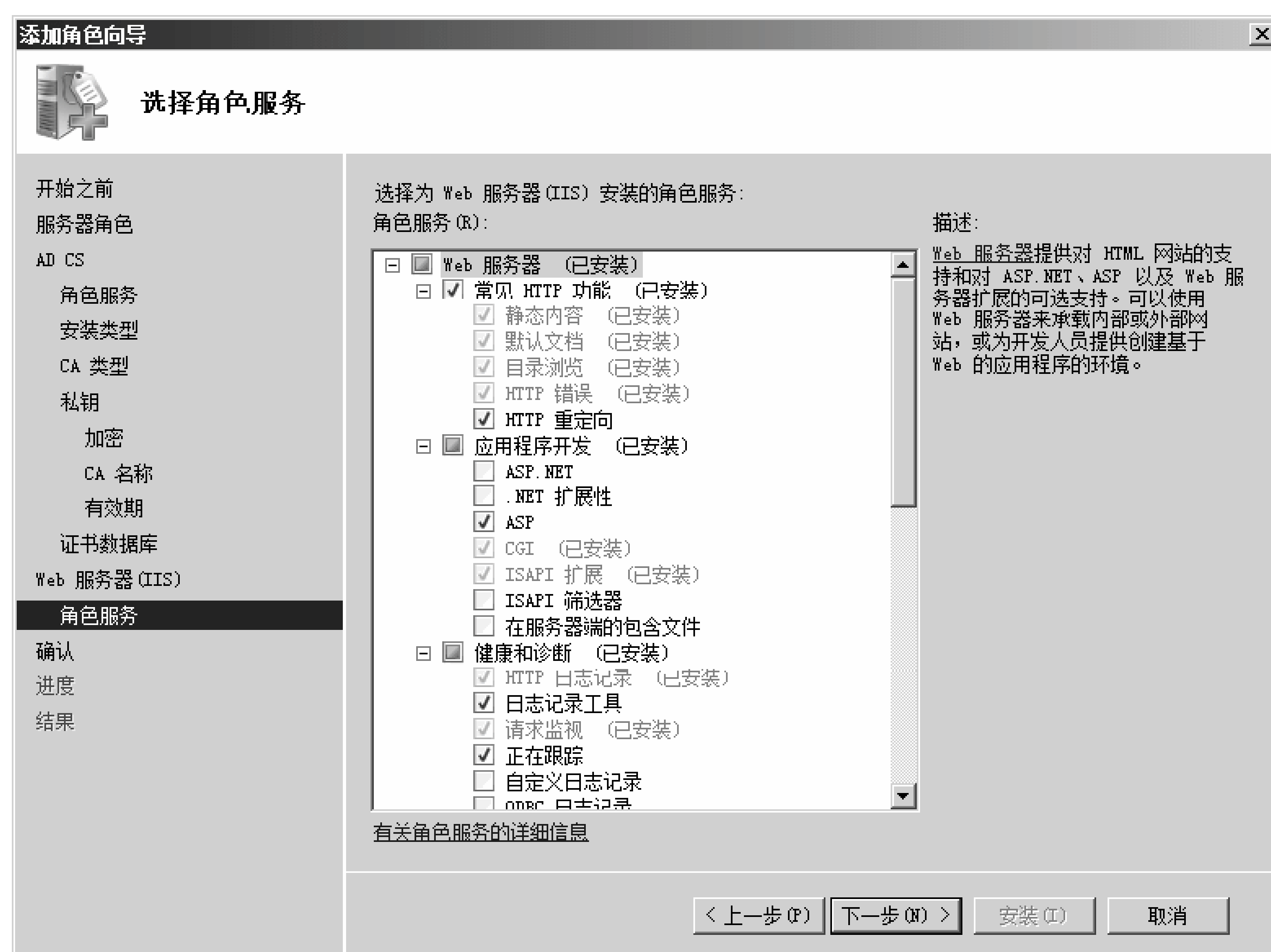


图 9-62　【选择角色服务】对话框



图 9-63　【确认安装选择】对话框

19 打开【安装进度】对话框，如图 9-64 所示，显示角色服务安装进度，并显示安装进度条。

20 打开【安装结果】对话框，证书服务安装完成，如图 9-65 所示，单击【关闭】按钮。



图 9-64　【安装进度】对话框

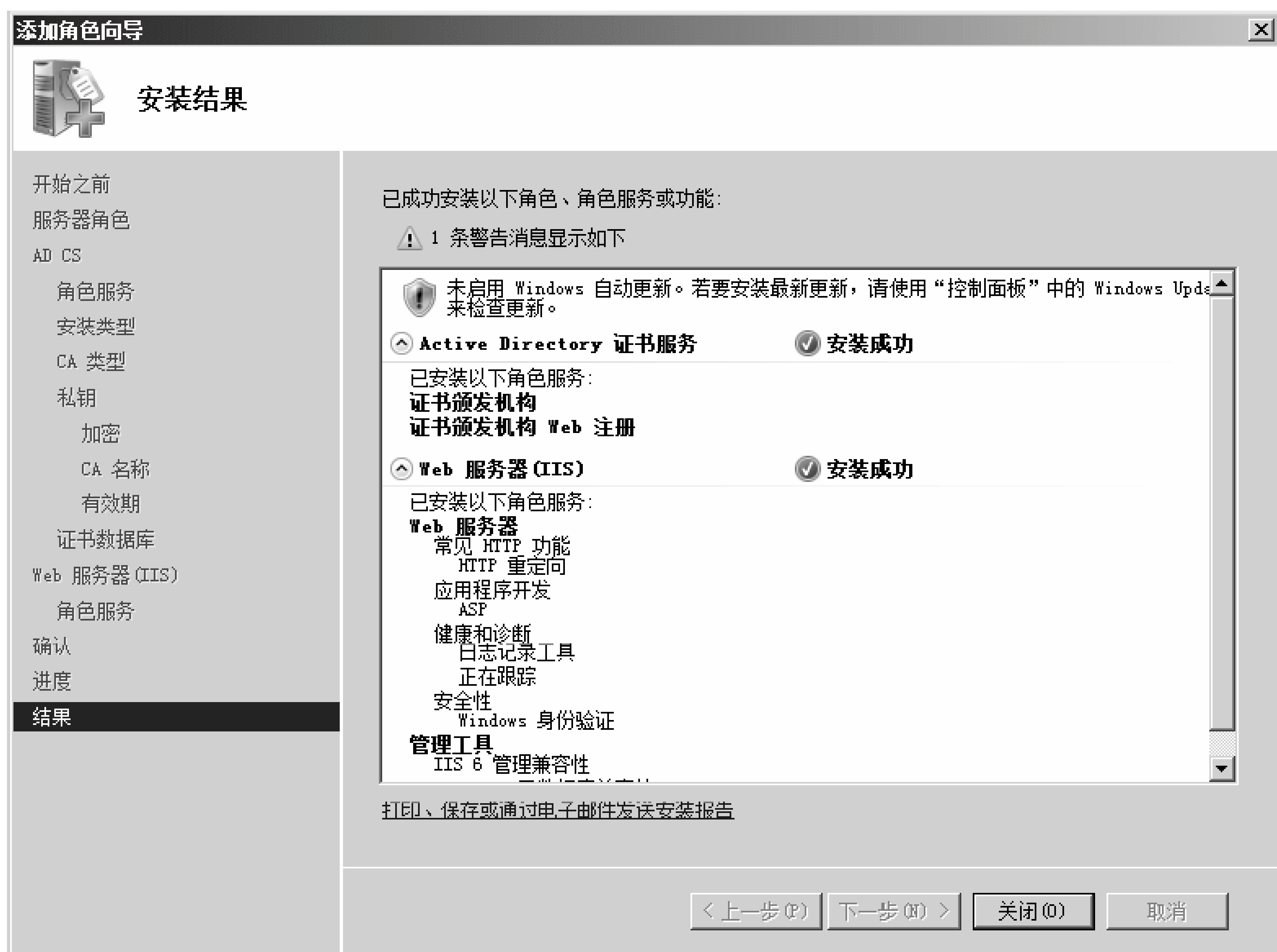


图 9-65　【安装结果】对话框

9.4.2　在 Web 服务器上制作证书申请文件并申请证书

在向 CA 证书颁发机构申请证书之前，需要先建立网站 Web 服务器的证书申请文件，网站的证书申请文件在网站 Web 服务器上进行操作，在 Web 服务器上制作证书申请文件的具体操作步骤如下。

01 在网站服务器上进行操作。右击【计算机】图标，在弹出的快捷菜单中选择【管理】命令。

02 打开【服务器管理器】窗口，选择【角色】➢【Web 服务器（IIS）】选项，如图 9-66 所示，单击【添加角色服务】链接。

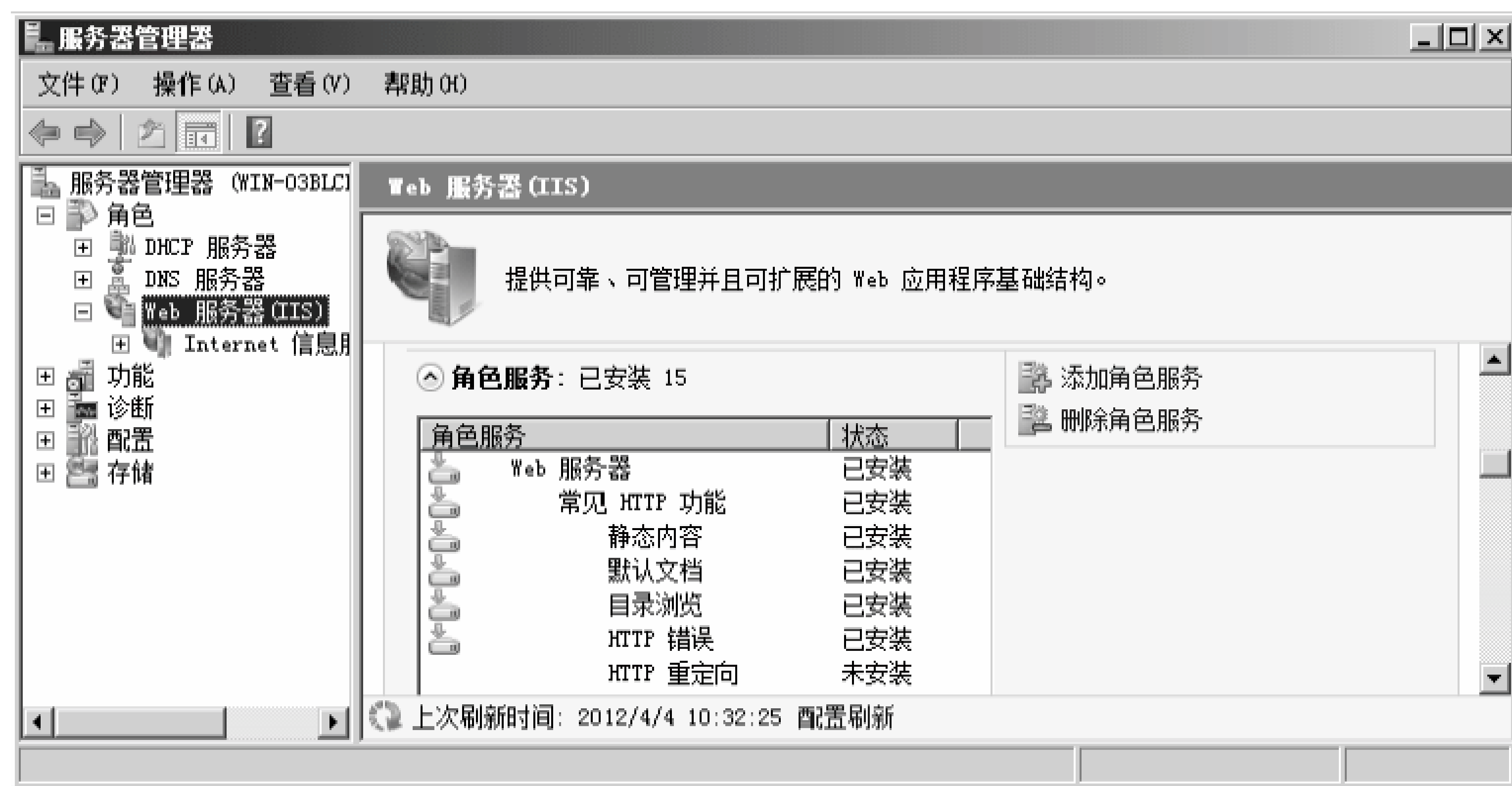


图 9-66　【服务器管理器】窗口

03 弹出【选择角色服务】对话框，如图 9-67 所示，选中【客户端证书映射身份验证】和【IIS 客户端证书映射身份验证】复选框，单击【下一步】按钮。

04 打开【确认安装选择】对话框，如图 9-68 所示，单击【安装】按钮。

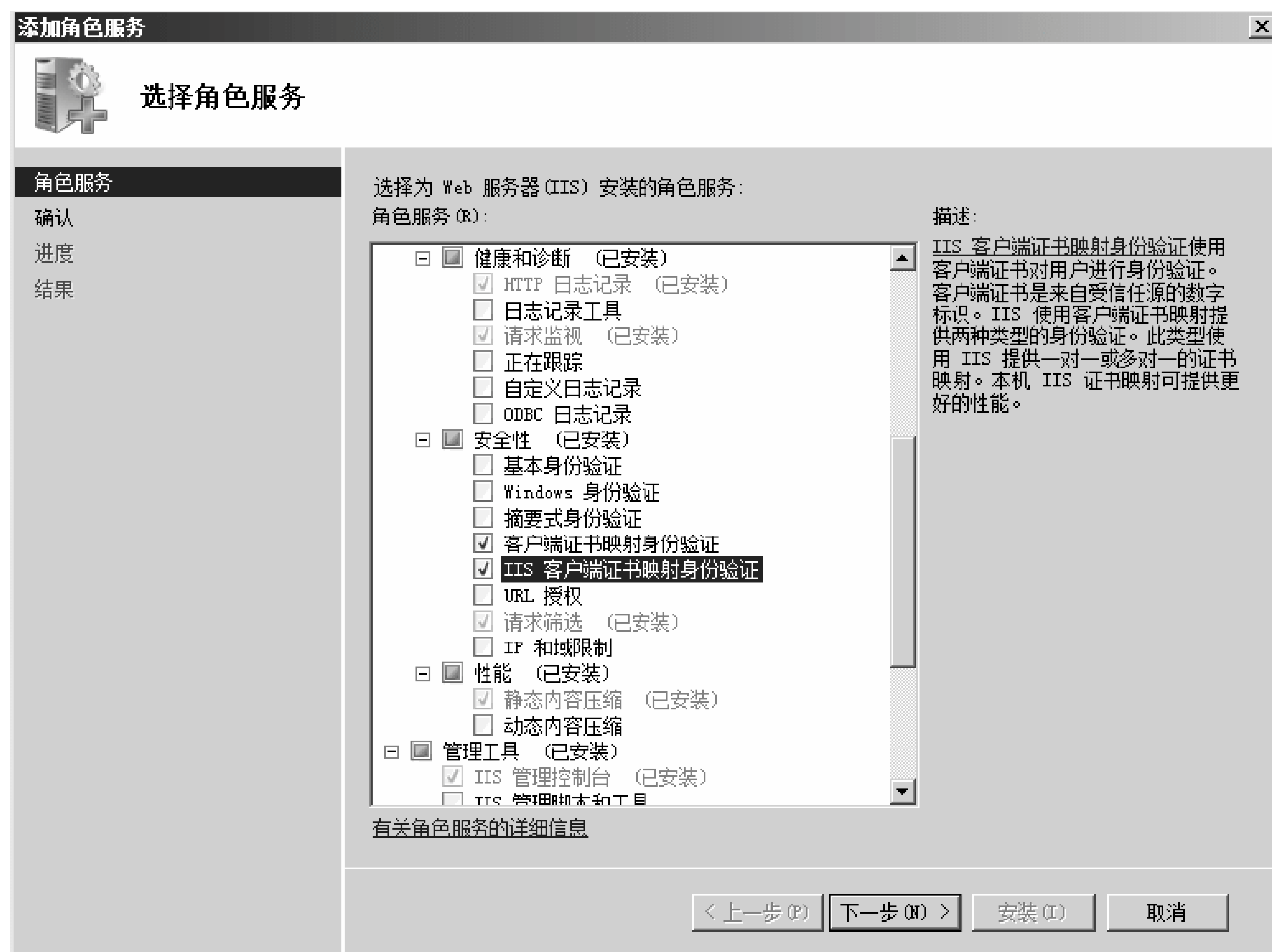


图 9-67　选择角色服务

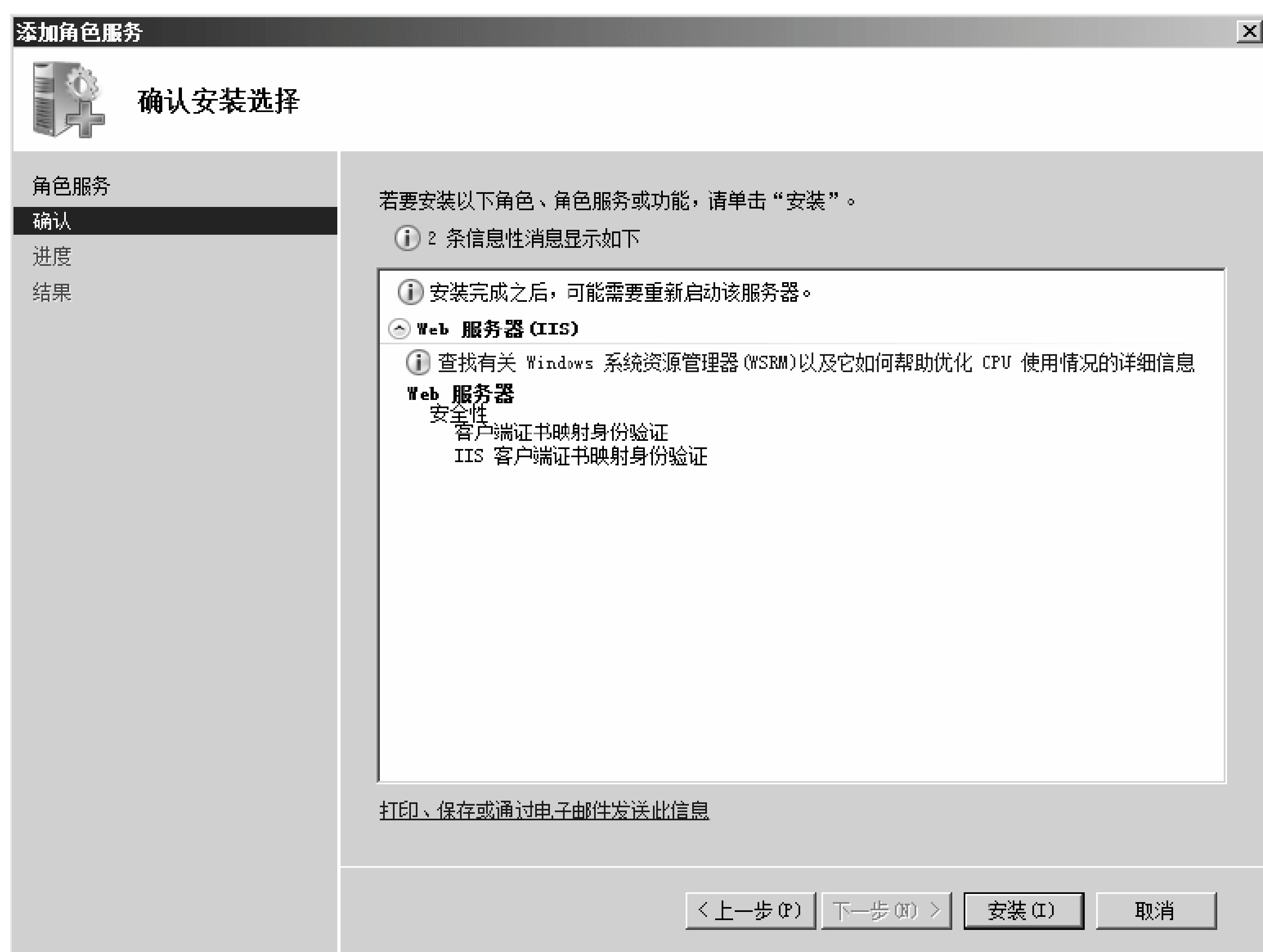


图 9-68　确认安装选择

05 打开【安装进度】对话框，如图 9-69 所示，显示 Web 服务器安全性安装进度，并显示安装进度条。

06 打开【安装结果】对话框，如图 9-70 所示，单击【关闭】按钮，完成 Web 服务器安全性的安装。



图 9-69　安装进度显示



图 9-70　安装结果

07 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，打开 Internet 信息服务管理器窗口，双击 WIN-013D26R8BJX 选项，双击【WIN-013D26R8BJX 主页】窗格中的【服务器证书】图标，如图 9-71 所示。

08 打开【服务器证书】对话框，单击右侧【创建证书申请】链接，如图 9-72 所示。



图 9-71 配置服务器证书

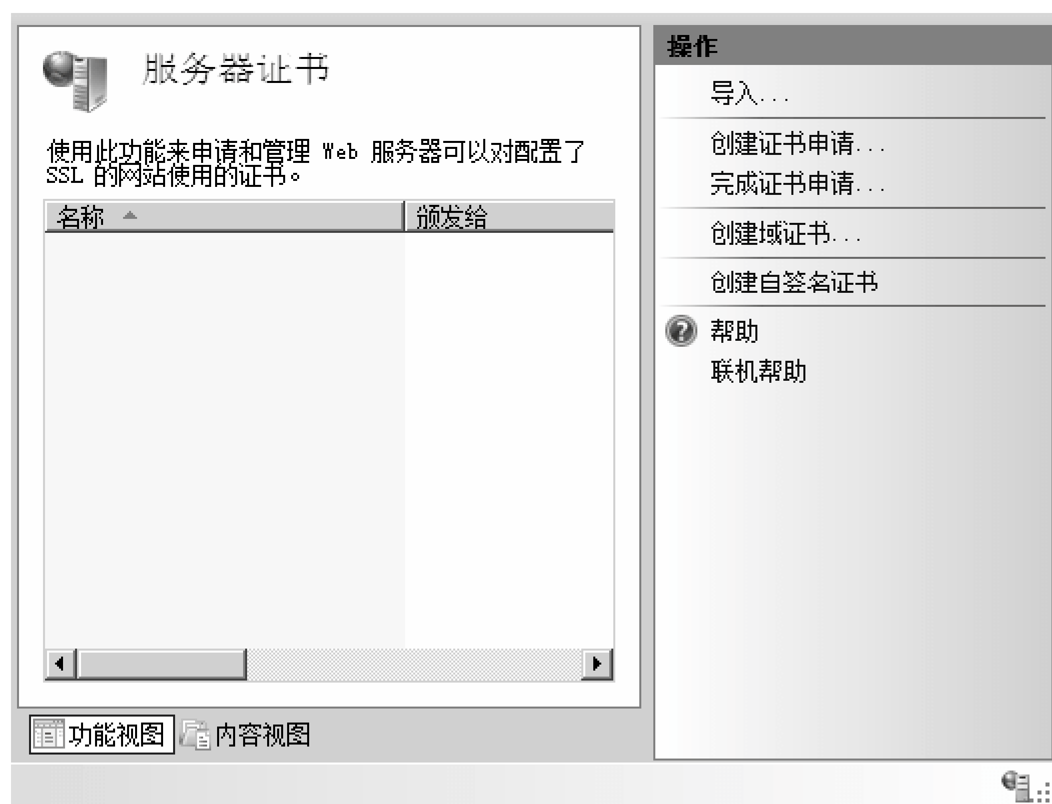


图 9-72 【服务器证书】对话框

09 弹出【证书申请】对话框，正确地填写证书所需信息，单击【下一步】按钮，如图 9-73 所示。

10 打开【加密服务】对话框，选择默认值，单击【下一步】按钮，如图 9-74 所示。



图 9-73 指定证书的必需信息



图 9-74 加密服务提供程序

11 打开【文件名】对话框，在【为证书申请指定一个文件名】文本框中输入证书的物理存放路径及名字，如图 9-75 所示，本实例为“C:\Users\Administrator\Desktop\asp.txt”，单击【完成】按钮，此时该 Web 服务器证书申请文件“asp.txt”创建完成。

12 如图 9-76 所示，打开 IE 浏览器，在地址栏输入 http://192.168.1.166/Certserv，其中“192.168.1.166”为 CA 证书服务器的 IP 地址，按 Enter 键，单击【申请证书】链接。



图 9-75 【文件名】对话框



图 9-76 访问 CA 服务器网站

13 打开【申请一个证书】页面，如图 9-77 所示，单击【高级证书申请】链接。

14 打开【高级证书申请】页面，如图 9-78 所示，单击【使用 base64 编码】链接。



图 9-77 【申请一个证书】页面

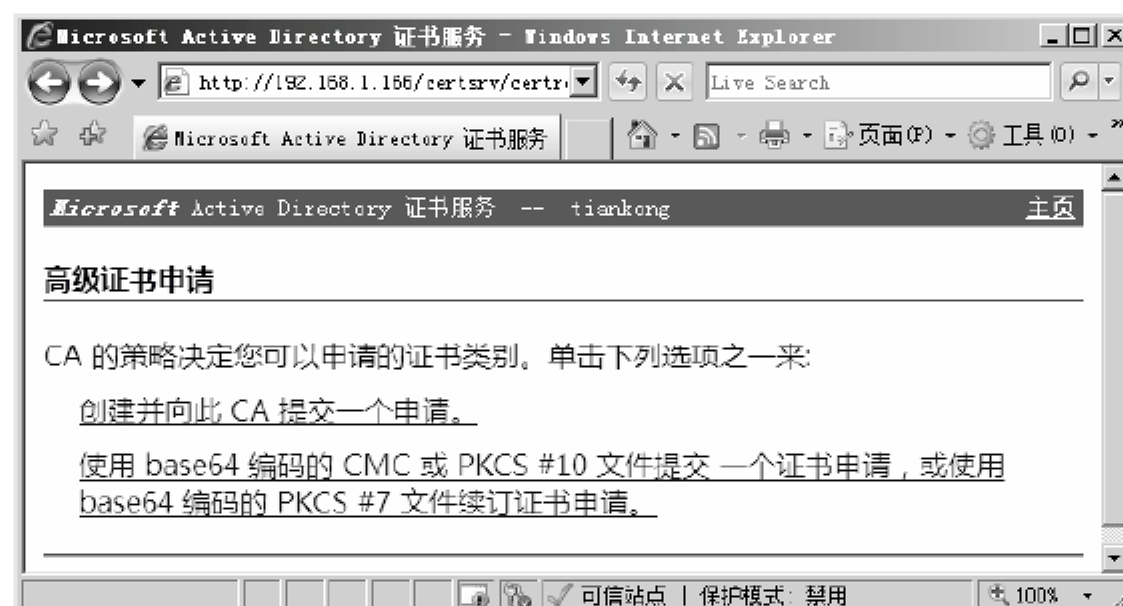


图 9-78 【高级证书申请】页面

15 打开证书申请提交页面，将已建立的证书申请文件“asp.net”中的所有内容复制到如图 9-79 所示位置，单击【提交】按钮。

16 打开【证书正在挂起】页面，如图 9-80 所示，表示证书申请结束，等待 CA 证书颁发颁发证书。



图 9-79 证书申请提交页面



图 9-80 【证书正在挂起】页面

9.4.3 CA 颁发证书

Web 服务器向证书颁发机构 CA 申请证书后，需要等待 CA 颁发证书。独立根 CA 需要管理员手工在 CA 服务器上颁发证书。手工颁发证书的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢ Certification Authority 选项，打开证书颁发机构窗口，在左侧选择 tiankong ➢【挂起的申请】选项，如图 9-81 所示，右侧显示有正在挂起的请求，右击该证书请求，在弹出的快捷菜单中选择【所有任务】➢【颁发】命令。

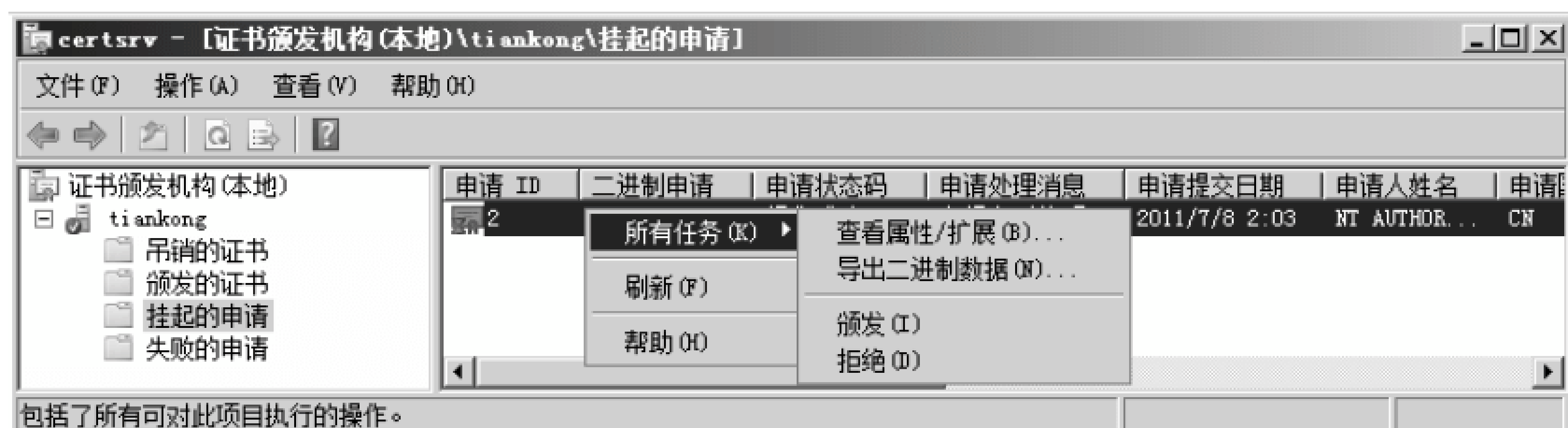


图 9-81 证书颁发机构窗口

02 返回至证书颁发结构窗口，如图 9-82 所示，选择【颁发的证书】选项，可以看到已经颁发过的证书。

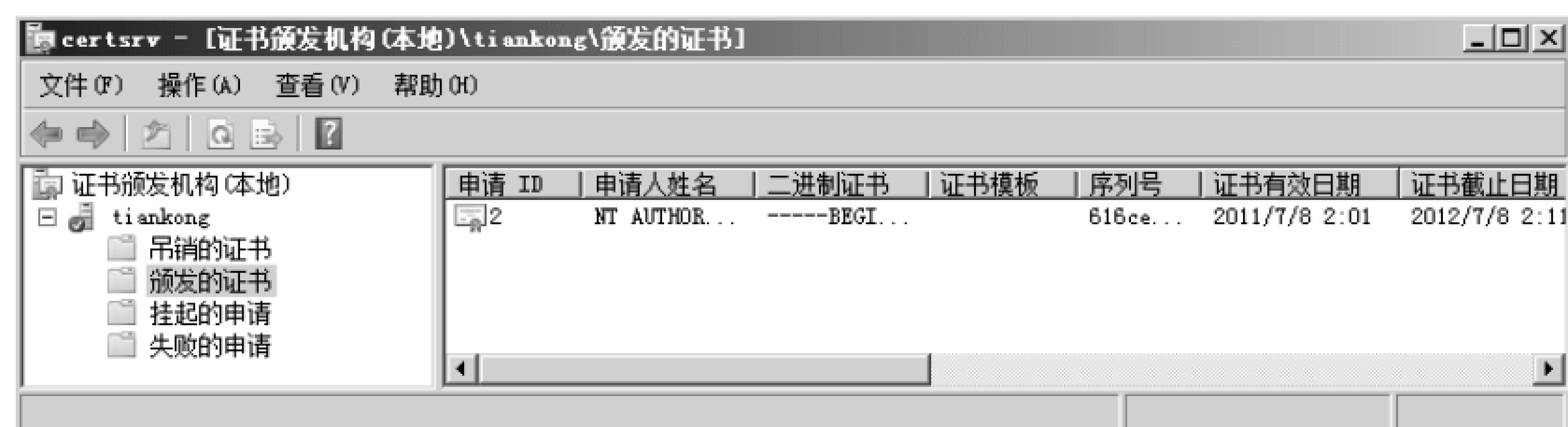


图 9-82 已颁发的证书

9.4.4 Web 服务器下载并安装证书

当 CA 颁发完证书后，Web 服务器需要访问证书颁发机构下载证书并进行安装。下载并安装证书的具体操作步骤如下。

01 打开 IE 浏览器，在地址栏输入"http://192.168.1.166/Certsrv"，其中"192.168.1.166"为 CA 证书服务器的 IP 地址，按 Enter 键，如图 9-83 所示，单击【查看挂起的证书申请的状态】链接。

02 打开【查看挂起的证书申请的状态】页面，如图 9-84 所示，单击【保存的证书申请】链接。

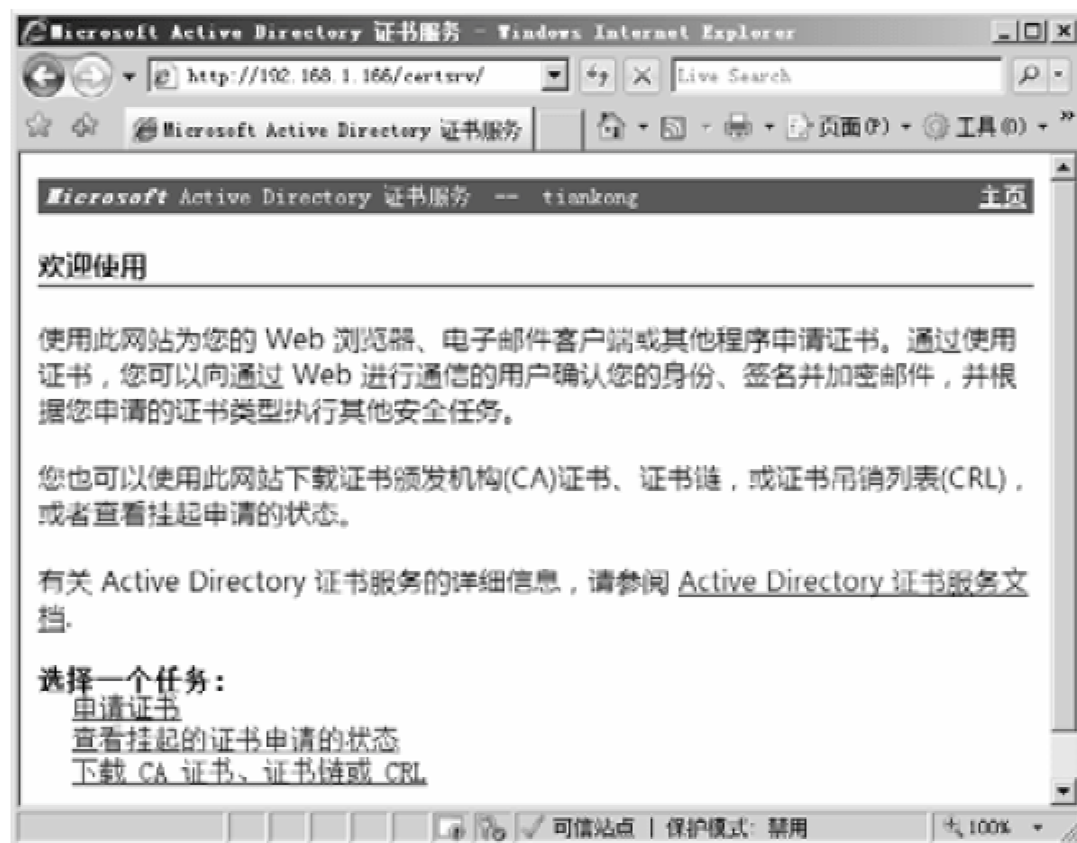


图 9-83　访问 CA 服务器网站

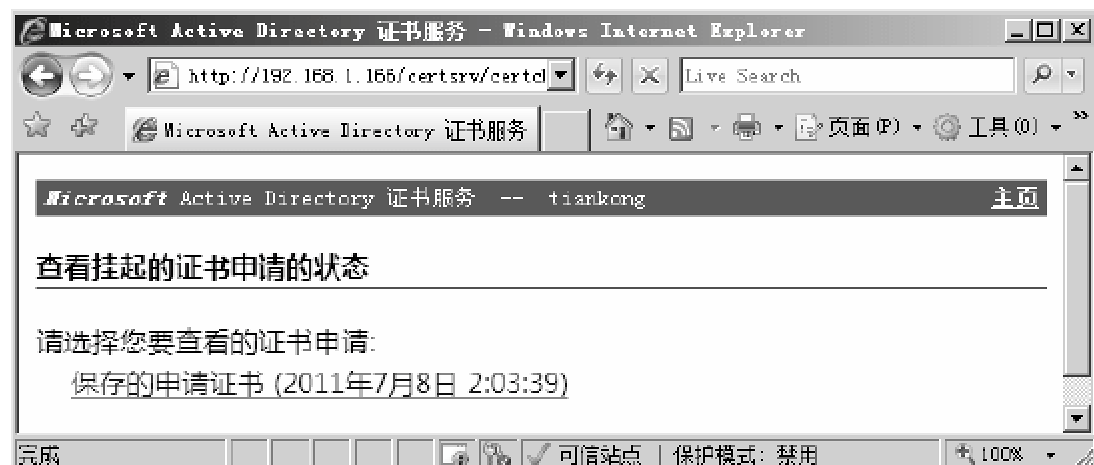


图 9-84　查看挂起的证书申请的状态

03 打开【证书已颁发】页面，如图 9-85 所示，选中【Base 64 编码】单选按钮，单击【下载证书】链接。

04 弹出【文件下载】提示框，如图 9-86 所示，单击【保存】按钮。

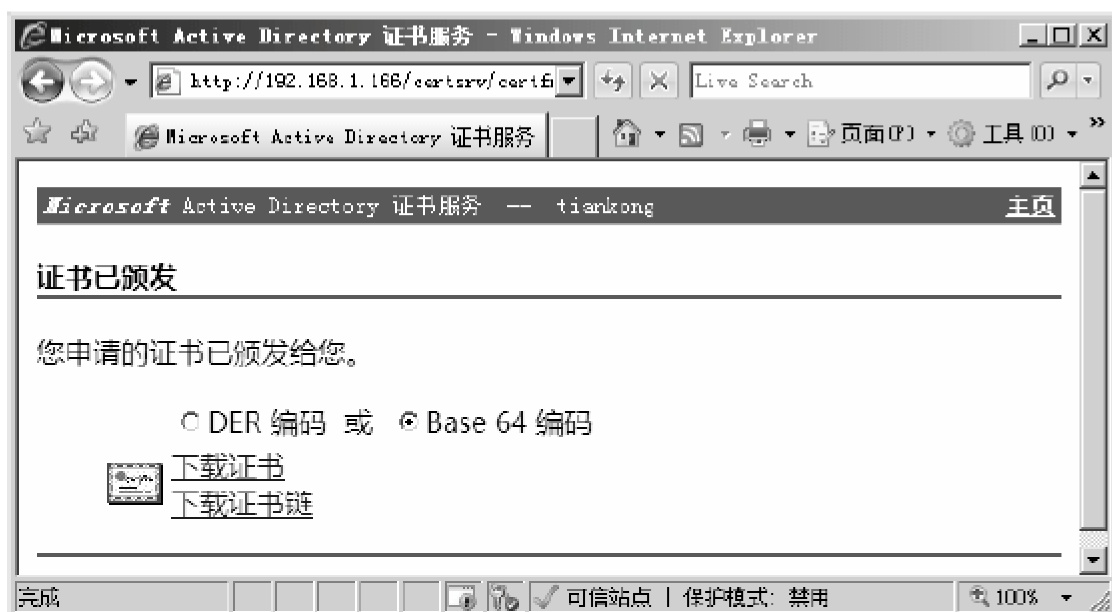


图 9-85　【证书已颁发】页面

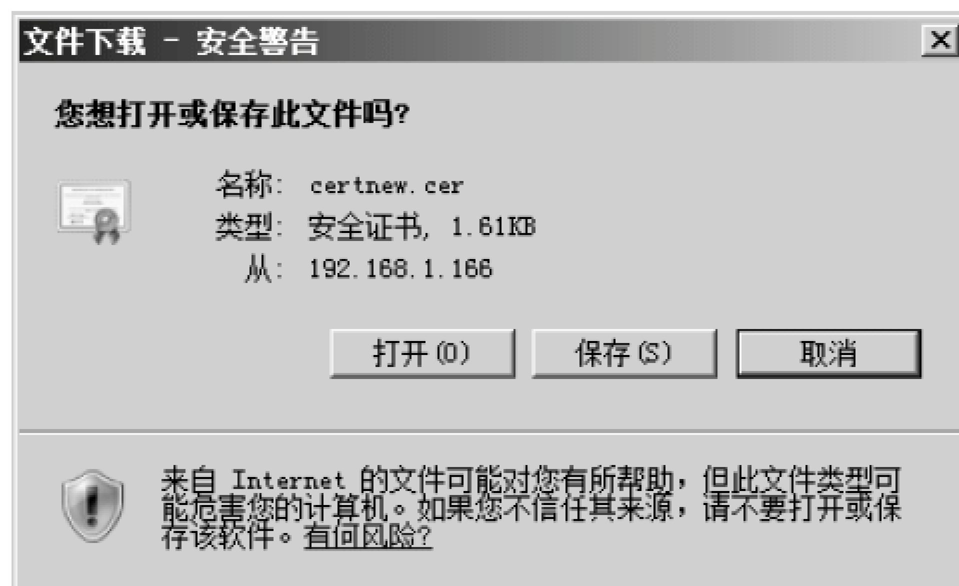


图 9-86　【文件下载】提示框

05 弹出【另存为】对话框，如图 9-87 所示，单击【浏览文件夹】按钮。



图 9-87　【另存为】对话框

06 弹出存放路径选择对话框，找到证书存放路径，如图 9-88 所示，本实例将证书存放在系统桌面上，单击【保存】按钮。

07 弹出【下载完毕】对话框，提示下载进度，如图 9-89 所示，下载证书文件结束，单击【关闭】按钮。

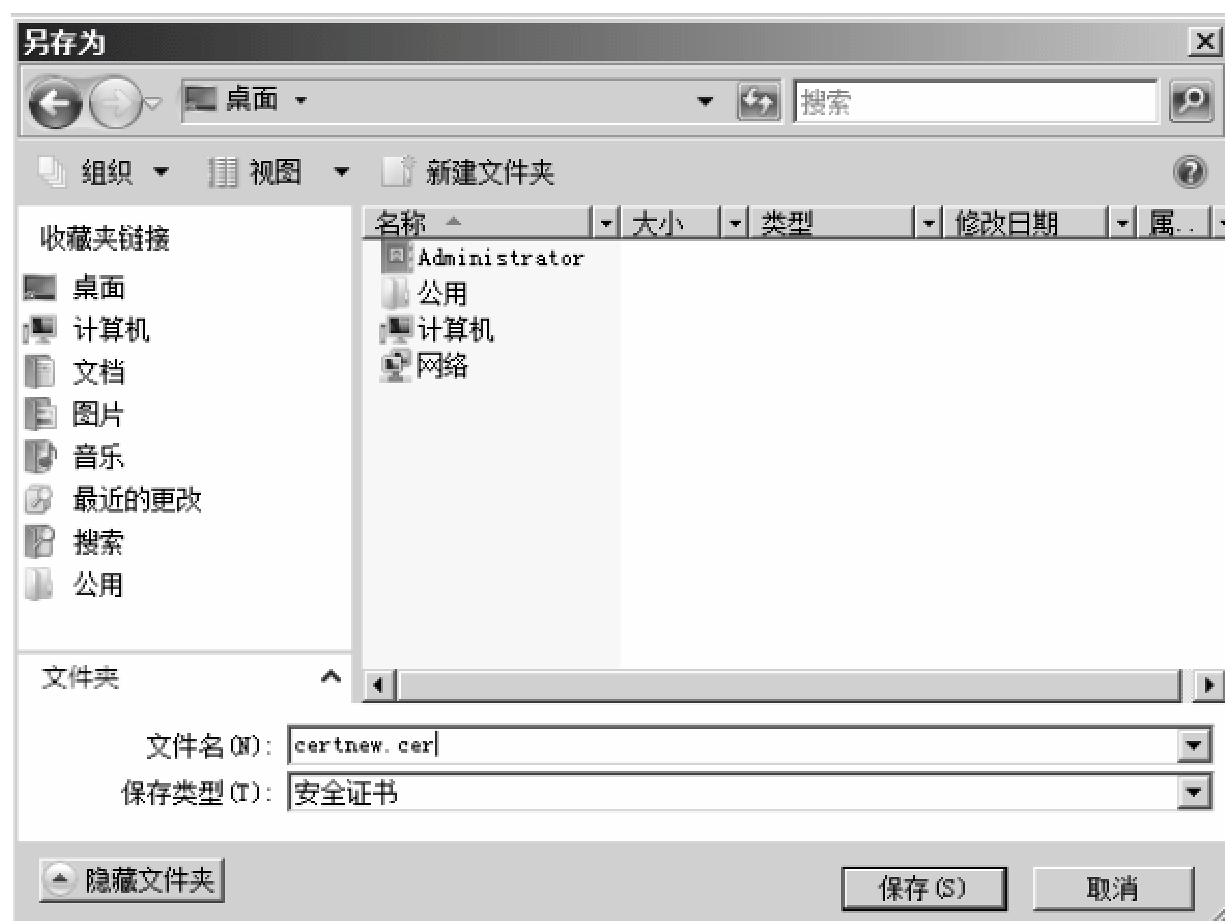


图 9-88　存放路径选择对话框

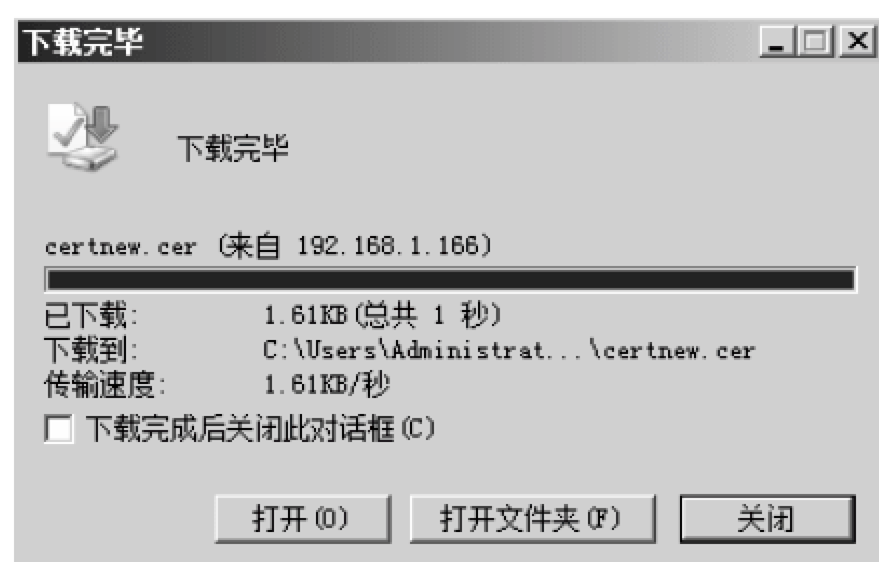


图 9-89　【下载完毕】对话框

08 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，弹出 Internet 信息服务管理器，选择 WIN-013D26R8BJX 选项，如图 9-90 所示，双击【WIN-013D26R8BJX 主页】窗格中的【服务器证书】图标。

09 打开【服务器证书】窗格，如图 9-91 所示，选择右侧【完成证书申请】选项。



图 9-90　选择【服务器证书】功能

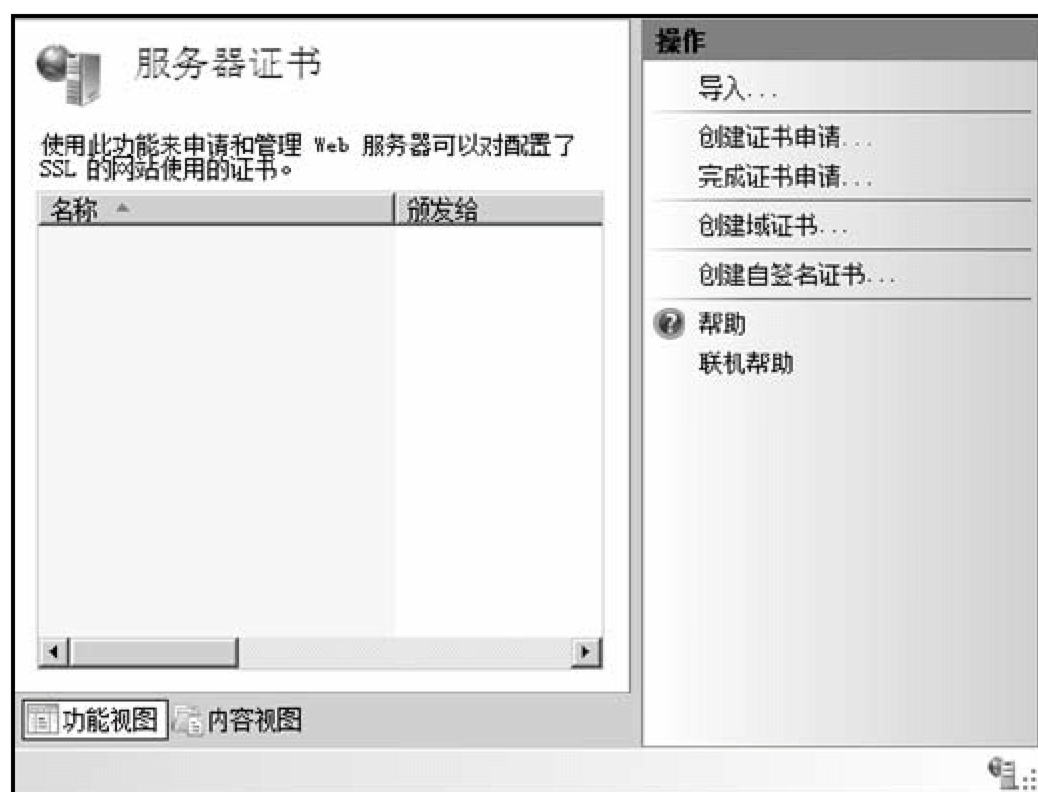


图 9-91　【服务器证书】窗格

10 弹出【指定证书颁发机构响应】对话框，在【包含证书颁发机构响应的文件名】文本框中输入证书的存放物理路径，本实例为“C: \Users\Administrator\Desktop\certnew.cer”，如图 9-92 所示，在【好记名称】文本框中输入名称为“asp”，单击【确定】按钮。

11 返回至 Internet 信息服务管理器窗口，如图 9-93 所示，可以看到证书导入服务器成功。

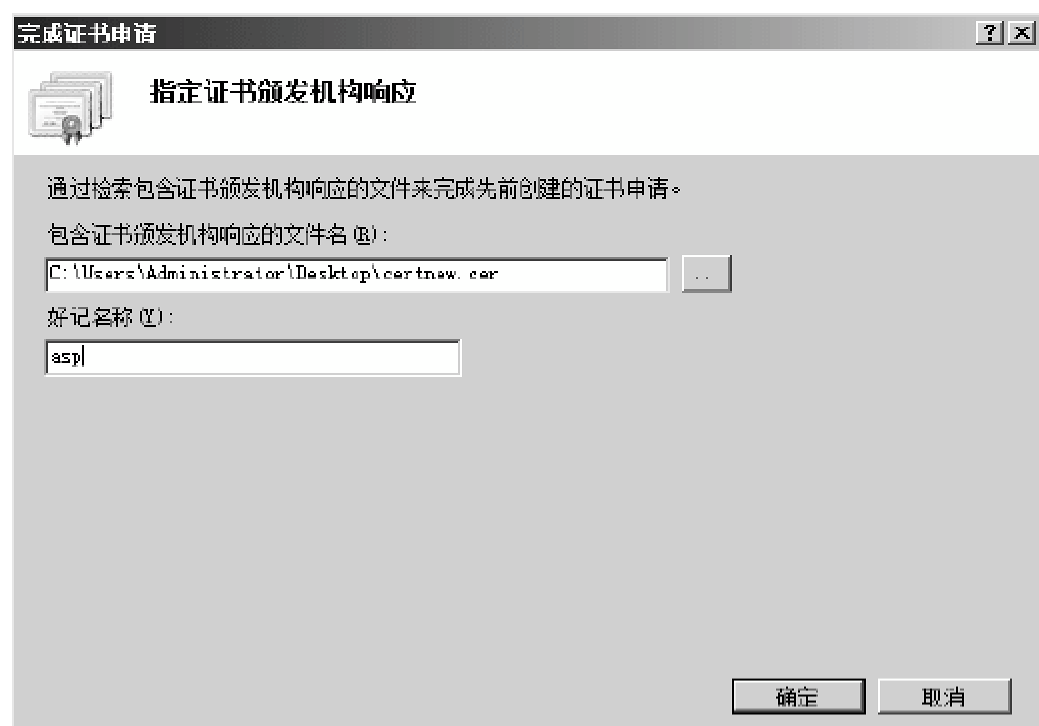


图 9-92　【指定证书颁发机构响应】对话框

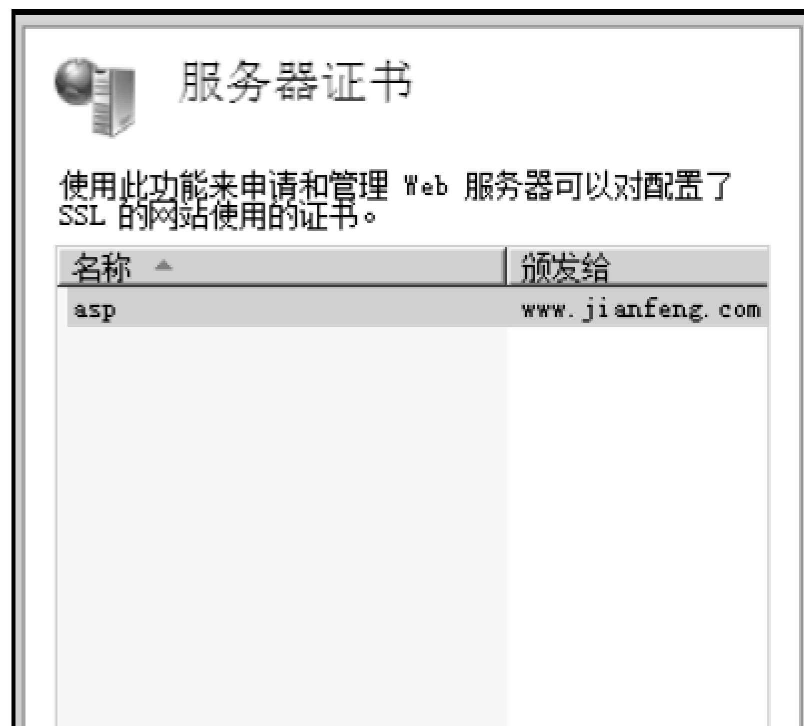


图 9-93　服务器证书添加成功

12 将 SSL 证书和网站进行绑定。选择要绑定的网站，选择 WIN-013D26R8BJX➢【网站】➢asp 选项，单击【asp 主页】窗格中的【SSL 设置】图标，然后选择右侧【操作】窗格中的【绑定】选项，如图 9-94 所示。

13 弹出【网站绑定】对话框，如图 9-95 所示，单击【添加】按钮。



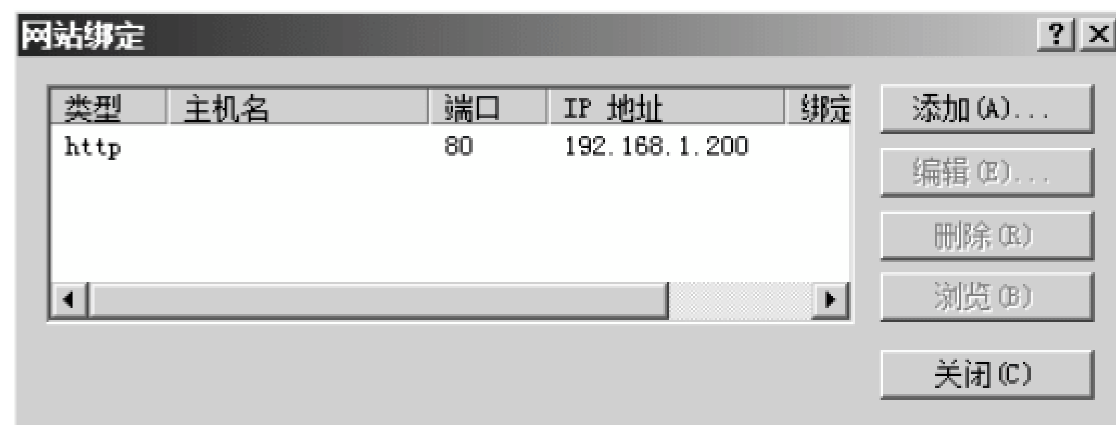


图 9-94　站点绑定　　　　图 9-95　【网站绑定】对话框

14 弹出【添加网站绑定】对话框，在【类型】下拉列表框中选择 https，在【SSL 证书】下拉列表框选择 asp 证书，如图 9-96 所示，单击【确定】按钮。

15 返回至【网站绑定】对话框，如图 9-97 所示，单击【关闭】对话框。



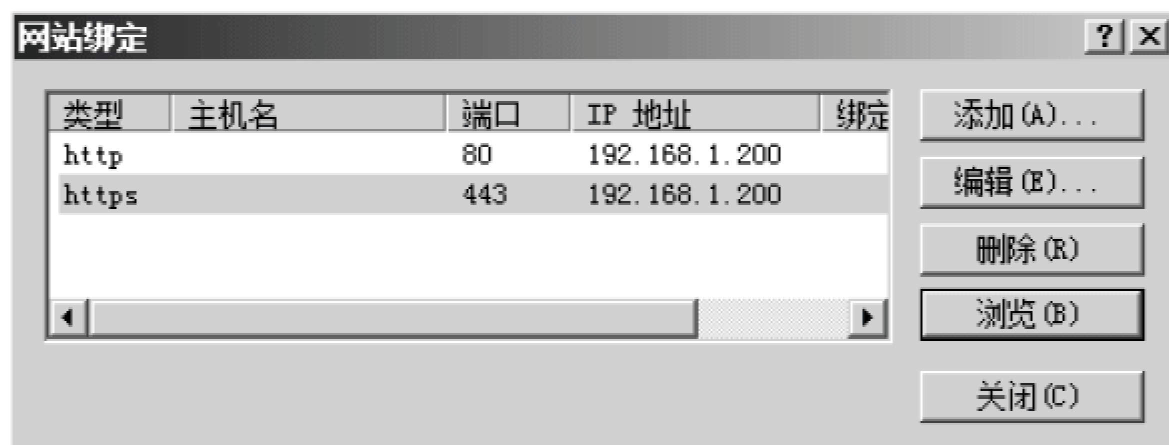


图 9-96　【添加网站绑定】对话框　　　　图 9-97　【网站绑定】对话框

16 返回至 Internet 信息服务管理器窗口，双击【asp 主页】窗格中的【SSL 设置】图标。

17 打开【SSL 设置】对话框，选中【要求 SSL】复选框，选中【客户证书】选项组的【忽略】单选按钮，如图 9-98 所示，选择右侧【应用】选项，至此 Web 服务器下载并安装证书结束。

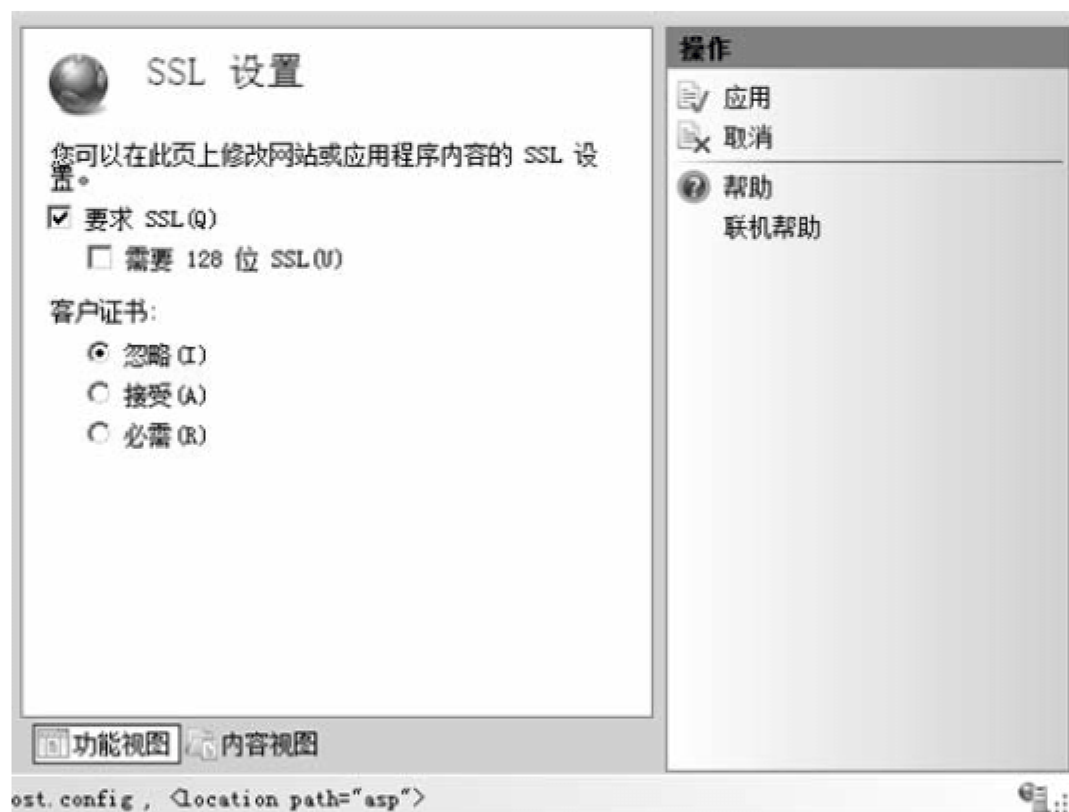


图 9-98 【SSL 设置】窗格

9.4.5 客户端信任 CA 安全访问网站

当网站安装证书并启用证书服务后，客户端就可以进行安全连接。但是客户端在访问 Web 服务器的时候需要将网址中的“http”修改为“https”。客户端访问启用 SSL 安全连接的 Web 服务器的具体操作步骤如下。

01 如图 9-99 所示，打开 IE 浏览器，在地址栏中输入“http: //www.jianfeng.com”，其中 www.jianfeng.com 为上文中启用 SSL 连接的 asp 网站，按 Enter 键，出现错误提示。

02 打开 IE 浏览器，在地址栏中输入“https: //www.jianfeng.com”，其中 www.jianfeng.com 为上文中启用 SSL 连接的 asp 网站，按 Enter 键，提示网站的安全证书有问题，原因是本实例中使用的证书是由自己架设的 CA 颁发的，IE 浏览器不信任此 CA 所致，如图 9-100 所示，单击【继续浏览此网站（不推荐）】链接。



图 9-99 访问启用 SSL 安全连接的网站 1

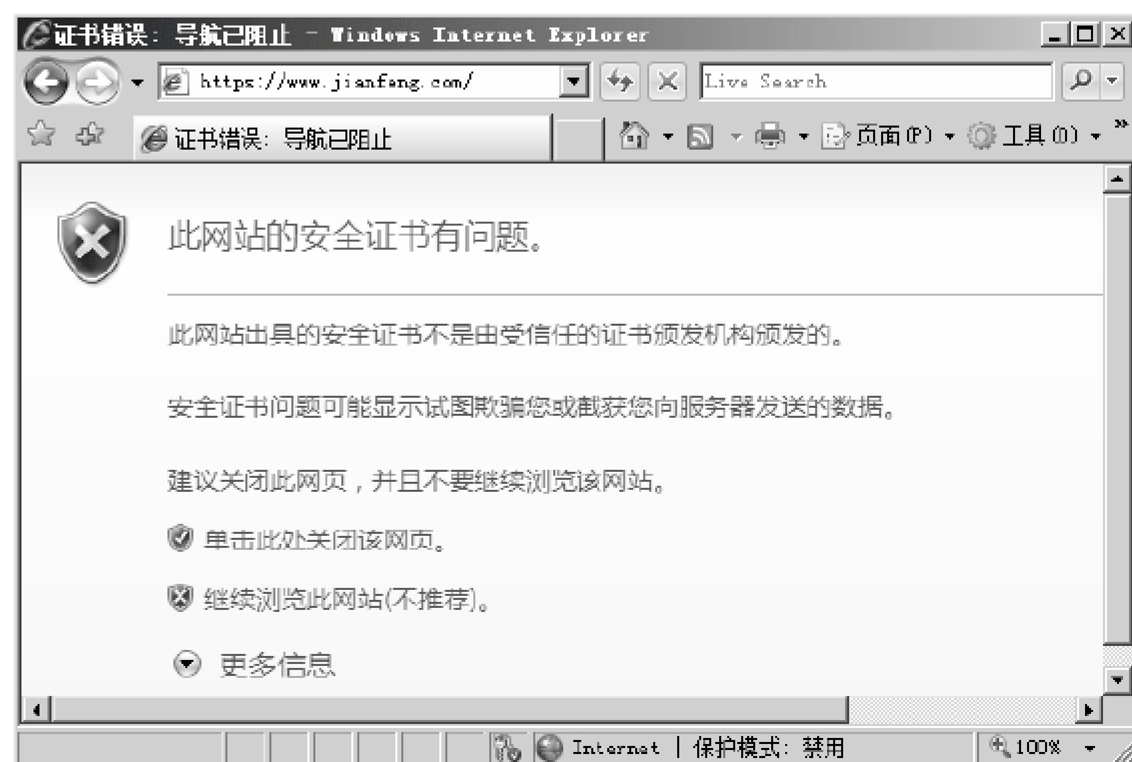


图 9-100 访问启用 SSL 安全连接的网站 2

03 弹出【安全警报】提示框，如图 9-101 所示，提示即将安全连接查看网页，单击【确定】按钮。

04 如图 9-102 所示，可以正确地浏览网页，但提示证书错误，这主要是该主机对证书颁发机构不信任。

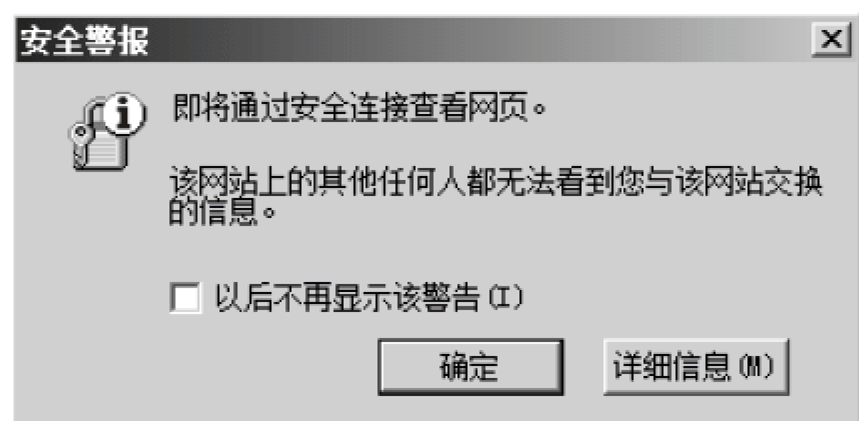


图 9-101 【安全警报】提示框



图 9-102 访问启用 SSL 安全连接的网站 3

05 信任 CA 证书颁发机构，安全打开网页。打开 IE 浏览器，在地址栏输入“http://192.168.1.166/certsrv”其中“192.168.1.166”为 CA 证书服务器的 IP 地址，按 Enter 键，打开证书服务申请网页，如图 9-103 所示，单击【下载 CA 证书、证书链或 CRL】链接。

06 打开【CA 证书】网页，选中【Base 64】单选按钮，如图 9-104 所示，单击【下载 CA 证书链】链接。



图 9-103 访问 CA 服务器网站

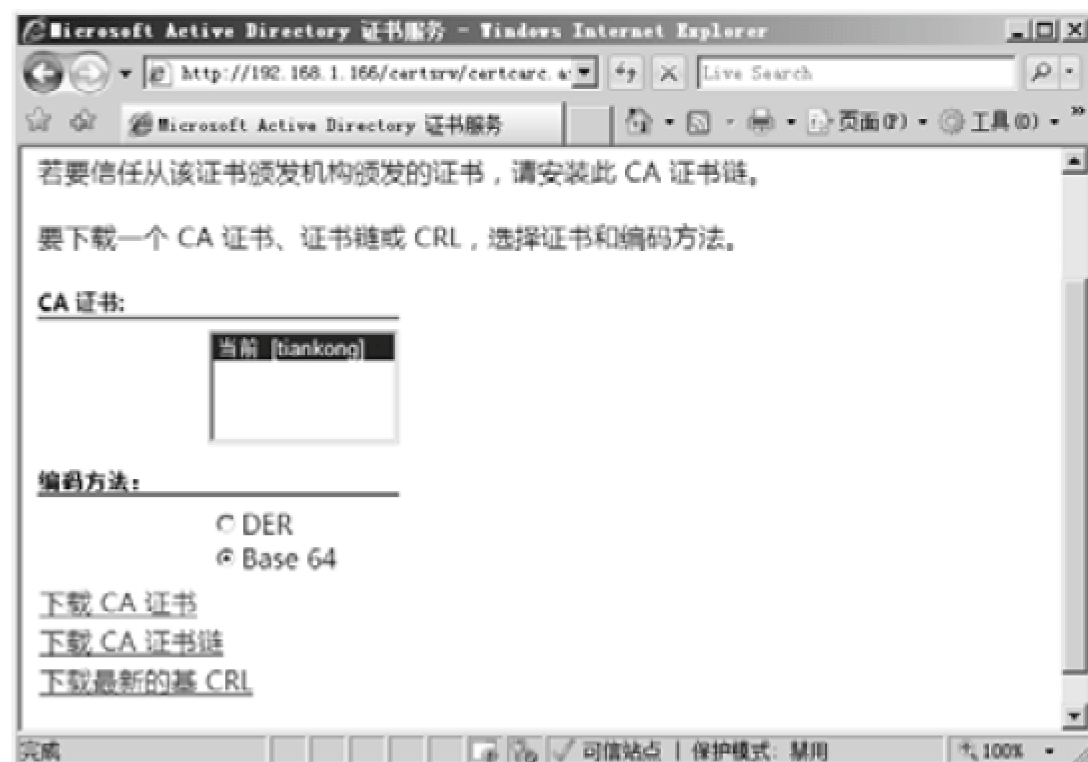


图 9-104 【CA 证书】页面

07 弹出【文件下载】提示框，如图 9-105 所示，单击【保存】按钮。

08 弹出【另存为】对话框，如图 9-106 所示，将证书的存储路径设置为桌面，单击【保存】按钮。

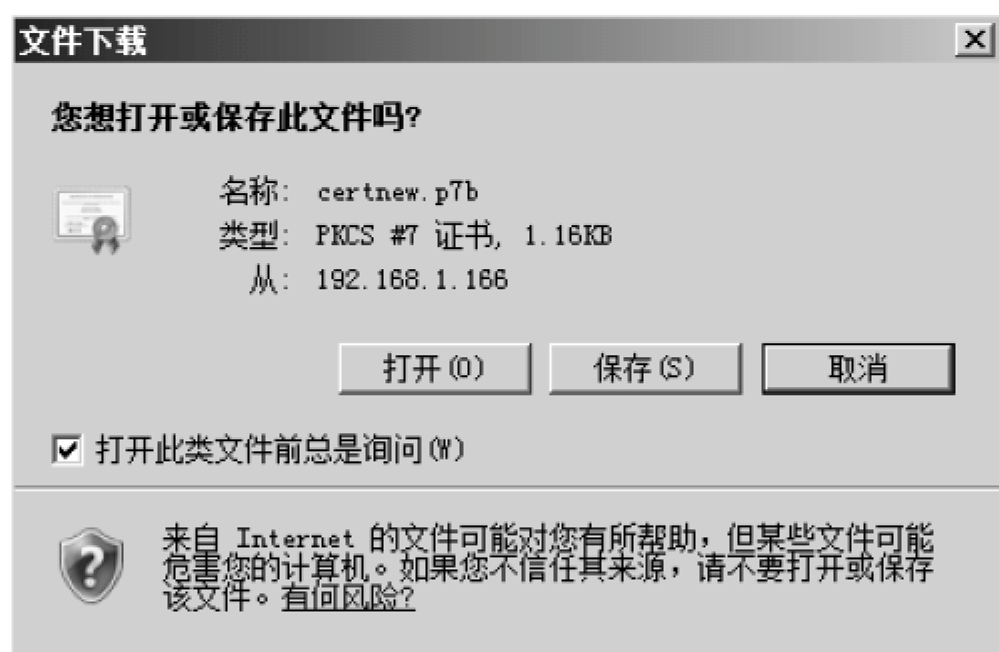


图 9-105 【文件下载】提示框

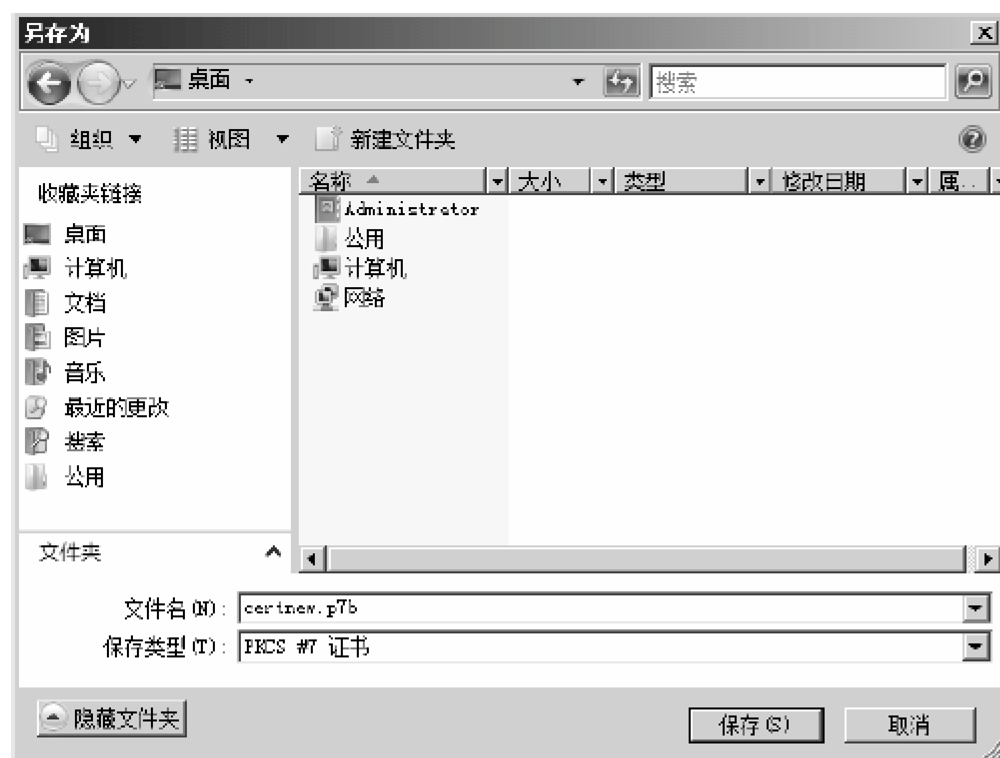


图 9-106 【另存为】对话框

09 弹出【下载完毕】对话框，如图 9-107 所示，单击【关闭】按钮。

10 在桌面上找到上一步骤下载的证书。如图 9-108 所示，右击证书，在弹出的快捷菜单中选择【安装证书】命令。

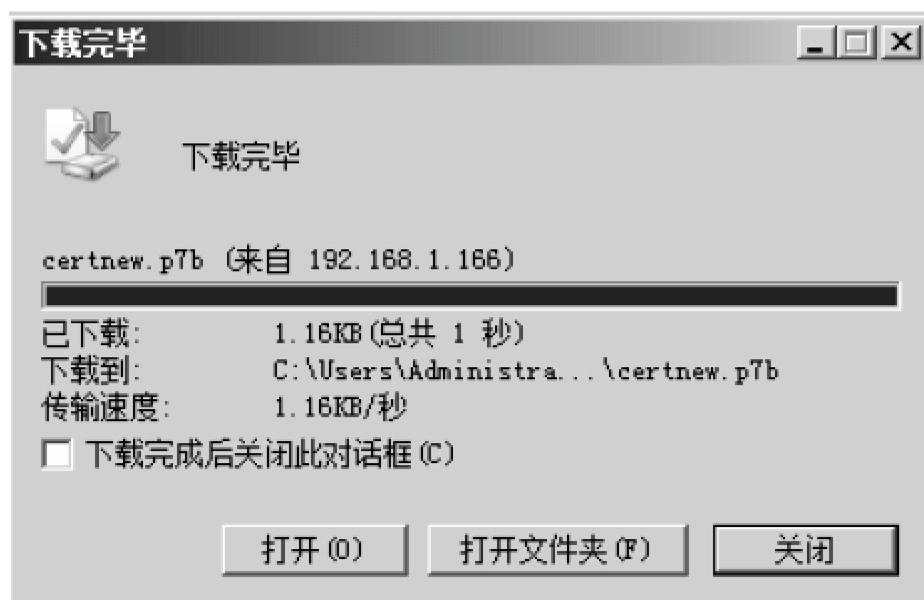


图 9-107 【下载完毕】对话框



图 9-108 安装证书

11 弹出【证书导入向导】对话框，如图 9-109 所示，单击【下一步】按钮。

12 弹出【证书存储】对话框，如图 9-110 所示，单击【下一步】按钮。

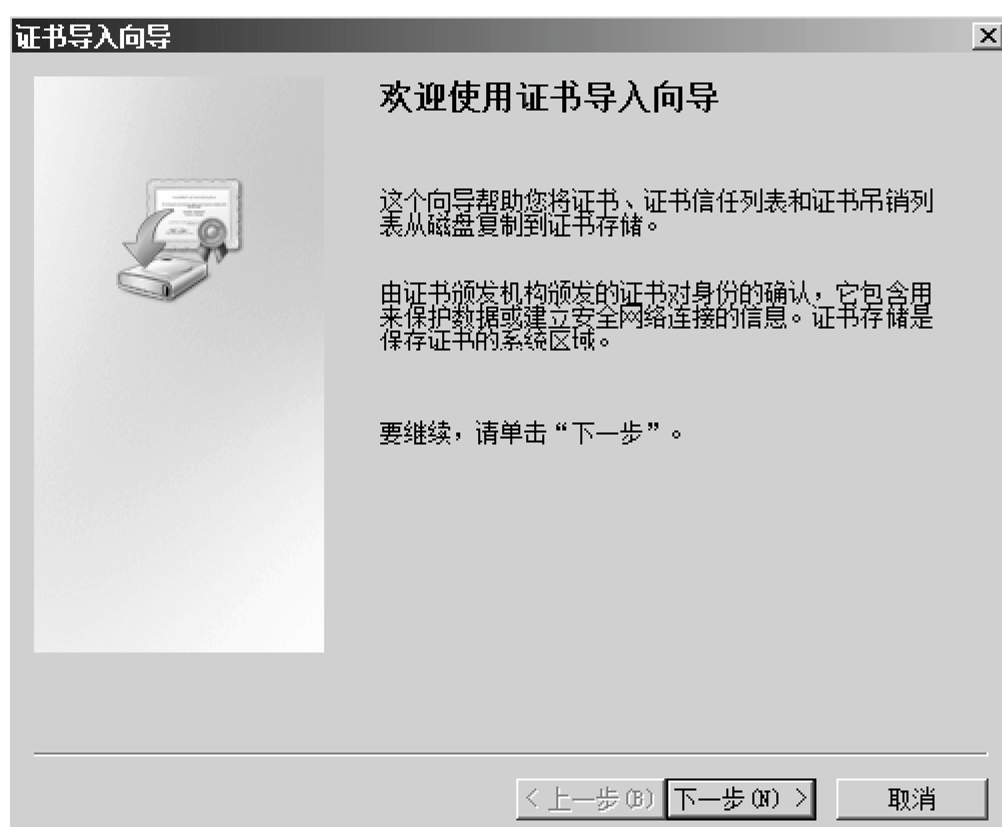


图 9-109 【证书导入向导】对话框

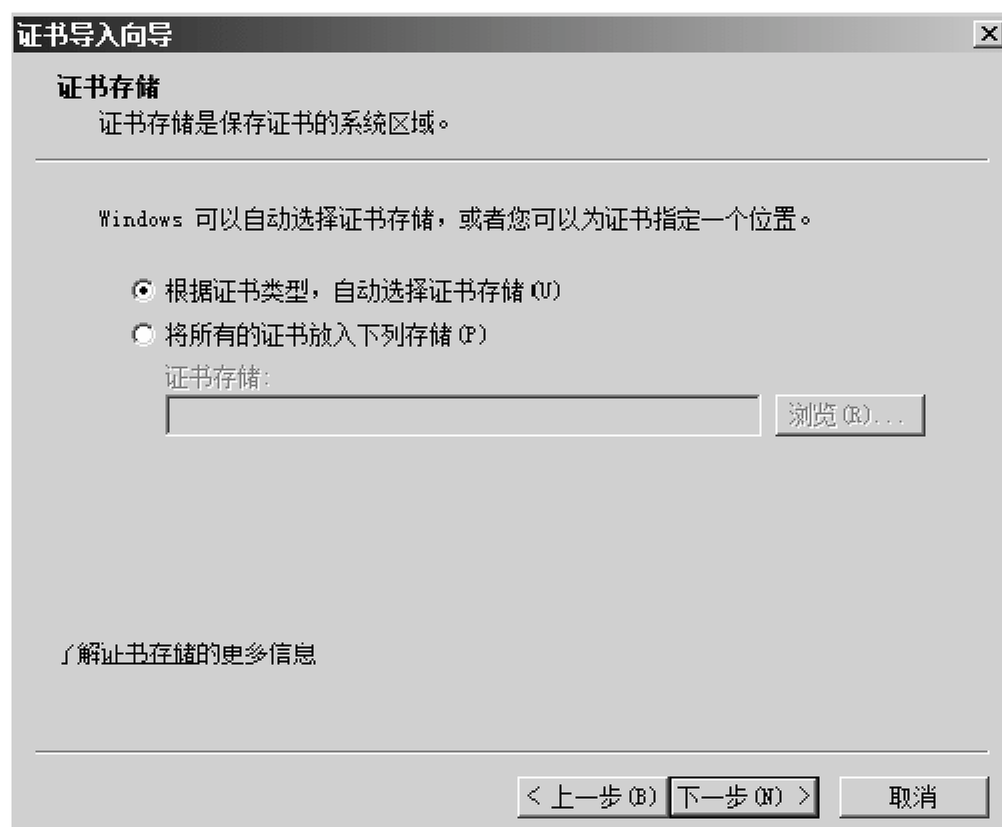


图 9-110 【证书存储】对话框

13 弹出完成证书导入对话框，如图 9-111 所示，单击【完成】按钮。

14 弹出【安全性警告】提示框，如图 9-112 所示，单击【是】按钮。

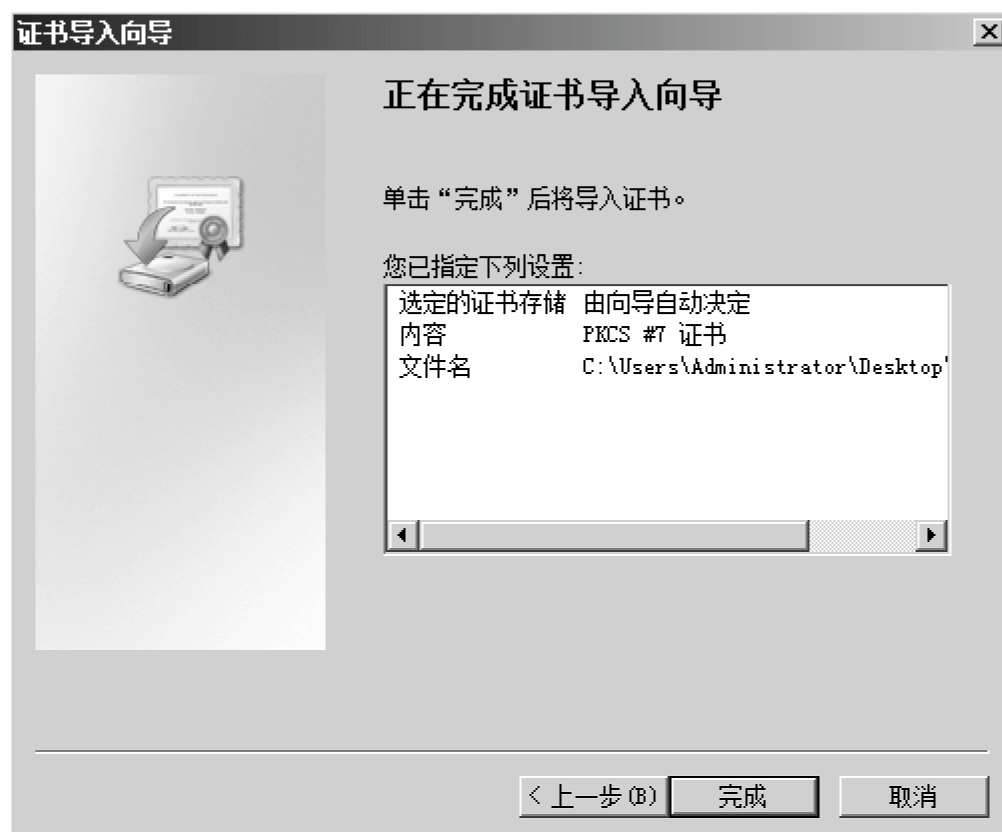


图 9-111　完成证书导入对话框

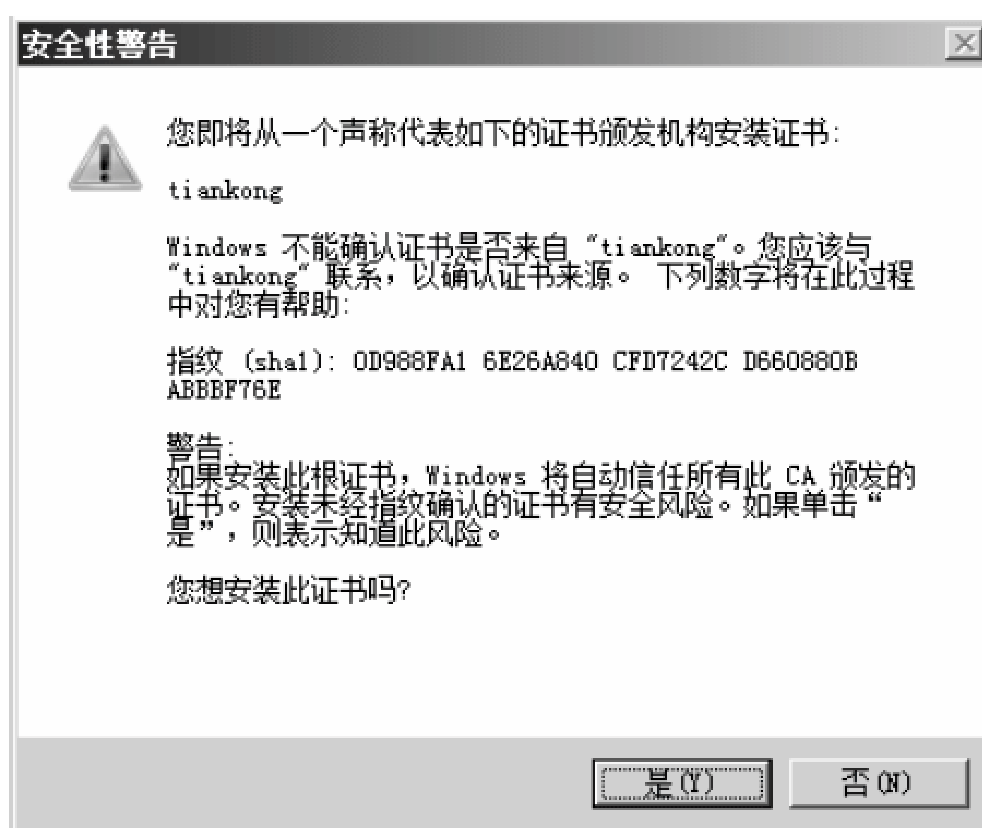


图 9-112　【安全性警告】提示框

15 弹出导入成功提示框，如图 9-113 所示，单击【确定】按钮。

16 如图 9-114 所示，打开 IE 浏览器，在地址栏中输入 “https: //www.jianfeng.com”，其中 “www.jianfeng.com” 为上文中启用 SSL 连接的 asp 网站，按 Enter 键。



图 9-113　导入成功



图 9-114　访问 asp 网站

17 弹出【安全警报】提示框，提示将通过安全连接查看网页，单击【确定】按钮。

18 如图 9-115 所示，正确打开网页。

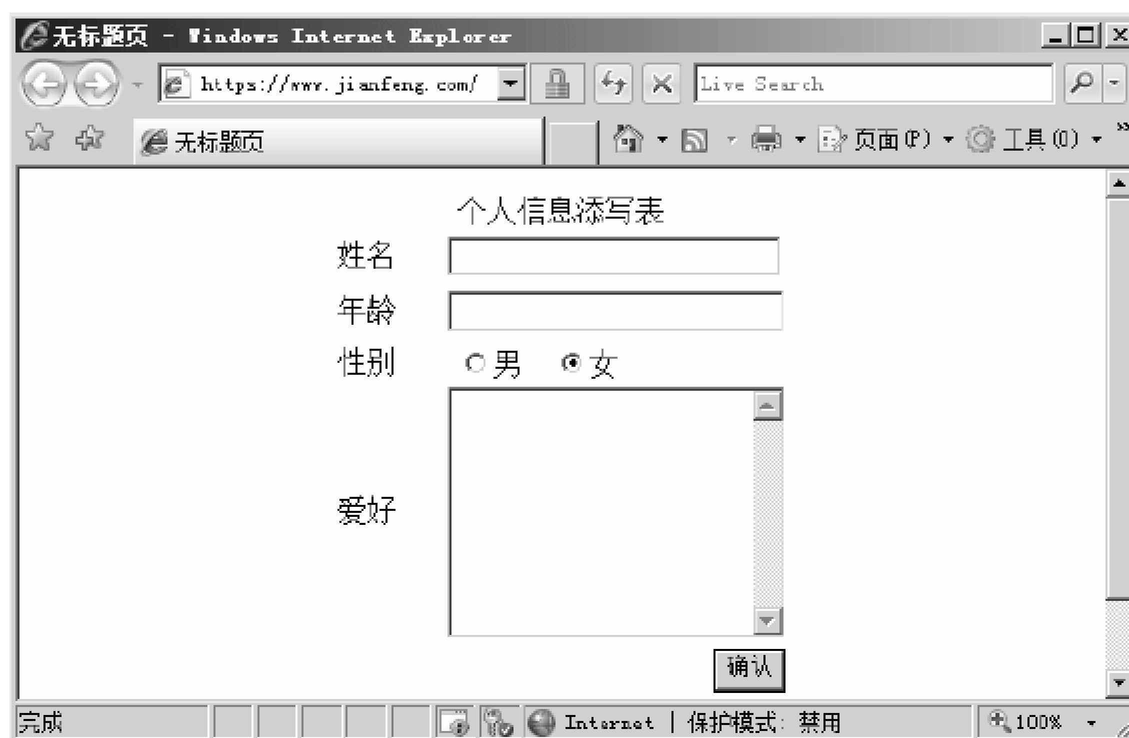


图 9-115　访问启用 SSL 网站 4

9.5 专家答疑

1. 使用 IIS 发布网站有多种方法，每种方法分别在什么场合使用？

答： 使用 IIS 发布网站共有三种不同的方法，他们的使用场合如下：

（1）使用不同的 IP 地址发布不同的网站。这种方法一个 IP 地址只发布一个网站，主要用在大型的商业网站和门户网站，另外政府网站往往也使用这种方法发布。

（2）使用同一个 IP 地址不同端口发布不同的网站。这种方法主要用在内部测试网站或者是网站的内页通过超链接访问使用。

（3）利用不同的主机头发布网站。这种方法又叫虚拟主机，为常用的网站发布方法。一般情况下中小型企业网站都采用这种方法，IDC 机房发布的网站常采用这种方法。

2. 是不是网站启用了证书之后数据传输就绝对安全？

答： 不是。安全是相对的，网站数据传输有了证书保护后，被截取的数据是加过密的，黑客要想看到这些数据必须首先解密才可以。但并不是说数据经过加密之后就不可以解密，黑客往往通过各种破解工具进行数据解密，所以养成良好的上网习惯，安全使用计算机才是关键。

第 10 章　发布企业动态网站

随着网站技术的发展，静态网站已经不能再满足市场的需求，越来越多的企业和机构采用了动态网站，目录主流的动态网站编程语言为 ASP.NET、JSP 和 PHP，下面详细讲解通过 IIS 发布企业动态网站的具体操作步骤。

10.1　发布 ASP.NET 动态网站

ASP.NET 是微软公司开发的一款编程语言，因为易学易用的特点，成为企业较为常用的网站编程语言之一，使用 IIS 发布 ASP.NET 动态网站的具体操作步骤如下。

10.1.1　安装 IIS 组件支持 ASP.NET

首先讲解如何安装和配置 ASP.NET 的动态环境，具体操作步骤如下。

01 右击【计算机】图标，如图 10-1 所示，在弹出的快捷菜单中选择【管理】命令。

02 弹出【服务器管理器】窗口，选择【角色】➢【Web 服务器（IIS）】选项，如图 10-2 所示，在右侧选择【添加角色服务】选项。

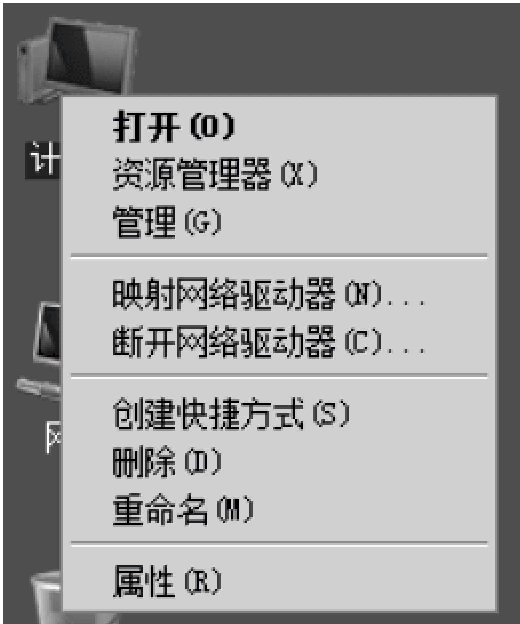


图 10-1　右击【计算机】图标



图 10-2　【服务器管理器】对话框

03 打开【选择角色服务】对话框，如图 10-3 所示，选中【应用程序开发】复选框。

04 弹出添加角色服务功能对话框，如图 10-4 所示，单击【添加必需的功能】按钮。

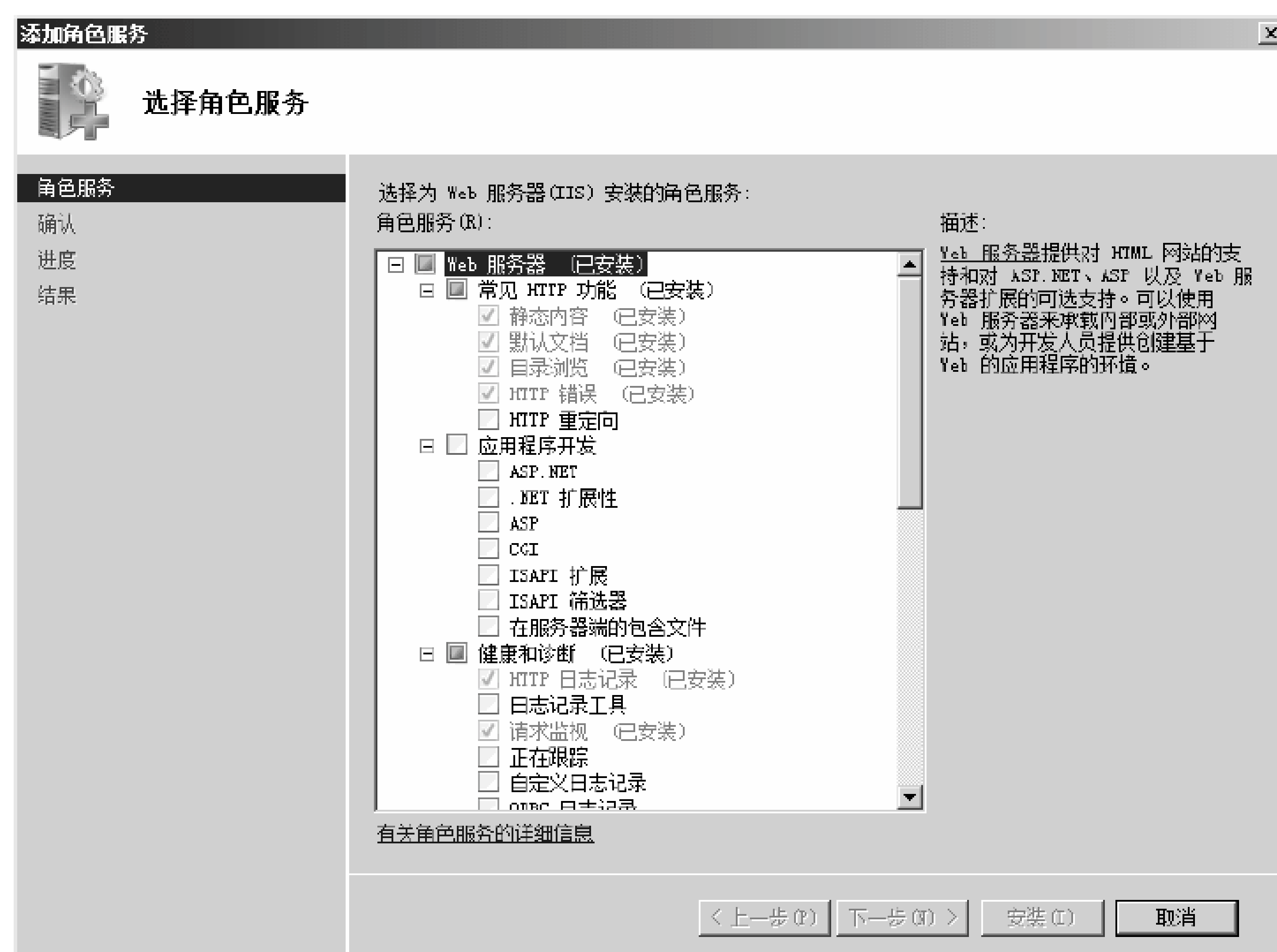


图 10-3 【选择角色服务】对话框

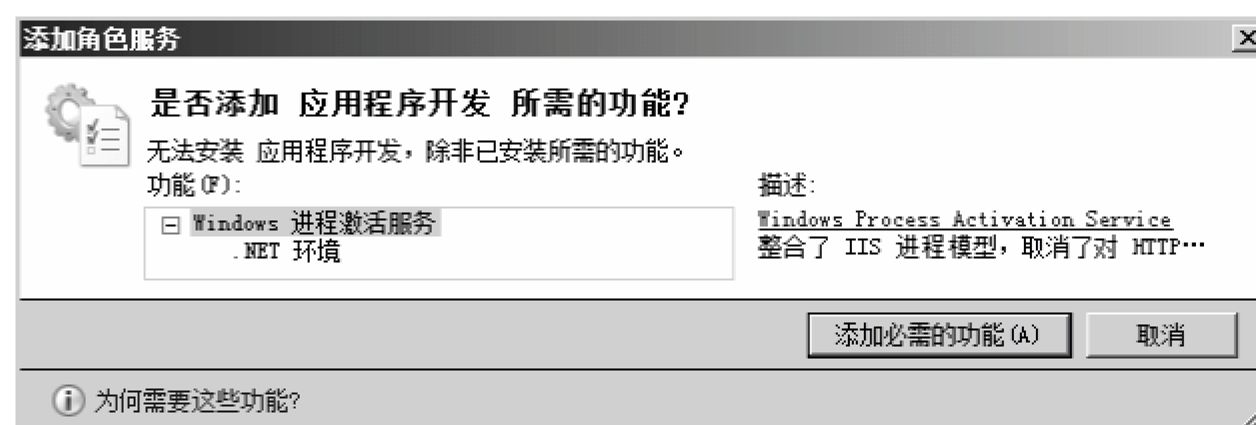


图 10-4 【添加角色服务功能】对话框

05 返回至【选择角色服务】对话框，如图 10-5 所示，单击【下一步】按钮。

06 打开【确认安装选择】对话框，如图 10-6 所示，单击【安装】按钮。

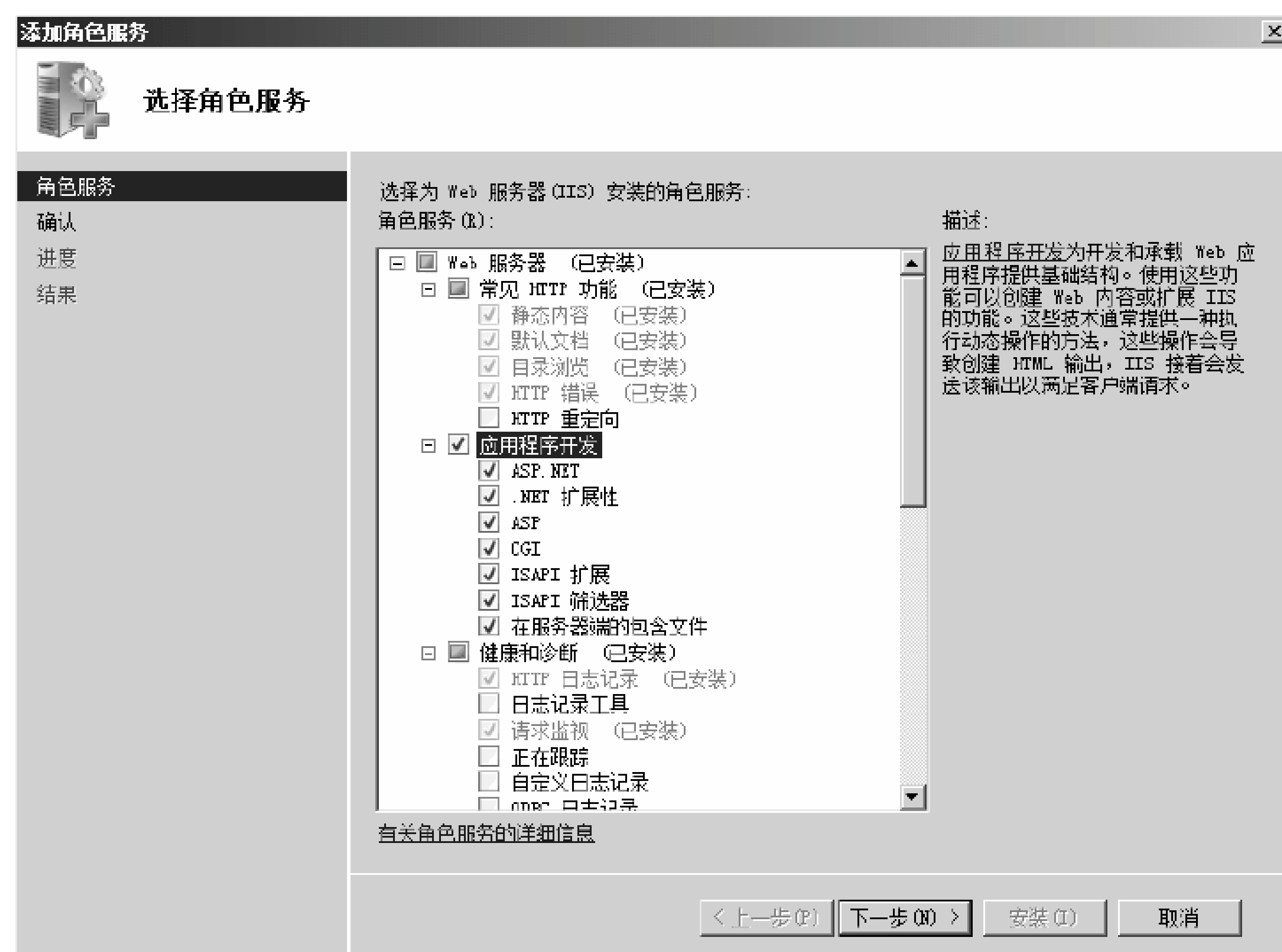


图 10-5 【选择角色服务】对话框



图 10-6　【确认安装选择】对话框

07 弹出【安装进度】对话框，如图 10-7 所示，显示角色服务安装进度，并显示安装进度条。

08 打开【安装结果】对话框，如图 10-8 所示，单击【关闭】按钮。



图 10-7　【安装进度】对话框



图 10-8　【安装结果】对话框

09 返回至【服务器管理器】窗口，至此支持 ASP.NET 环境的角色服务安装完成，如图 10-9 所示。



图 10-9　角色服务安装完成

10.1.2　网站发布

安装完 ASP.NET 动态环境之后就可以开始发布 ASP.NET 动态网站，本实例是在 IP 地址为“192.168.1.200”的 Web 服务器上发布域名为 www.jianfeng.com 的商业动态网站，具体的操作步骤如下。

01 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，弹出【Internet 信息服务（IIS）管理器】窗口，选择 WIN-013D26R8BJX，右击【网站】选项，在弹出的快捷菜单

中选择【添加网站】命令，如图 10-10 所示。



图 10-10　【Internet 信息服务（IIS）管理器】窗口

02 弹出【添加网站】对话框，在【网站名称】文本框中输入网站的名称，如图 10-11 所示，本实例为“asp”，单击【物理路径】文本框后面的 .. 按钮。

03 弹出【浏览文件夹】对话框，浏览找到网站 asp 的主目录的物理路径，如图 10-12 所示，本实例为“C:\asp”，单击【确定】按钮。

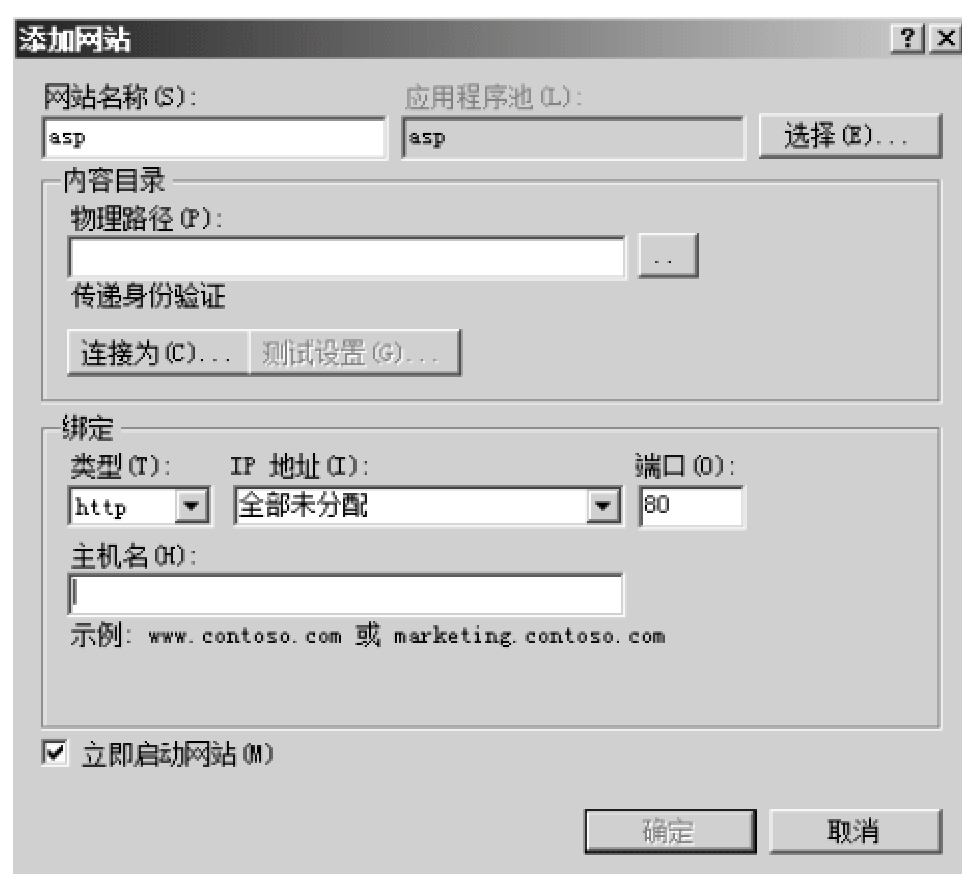


图 10-11　【添加网站】对话框



图 10-12　【浏览文件夹】对话框

04 返回至【添加网站】对话框，在【IP 地址】下拉列表框中选择 IP 地址为“192.168.1.200”，在【主机名】文本框中输入网站 asp 的域名，如图 10-13 所示，本实例为“www.jianfeng.com”，单击【确定】按钮。

05 返回至【Internet 信息服务（IIS）管理器】窗口，选择左侧 asp 选项，如图 10-14 所示，双击【asp 主页】窗格中的【默认文档】图标。

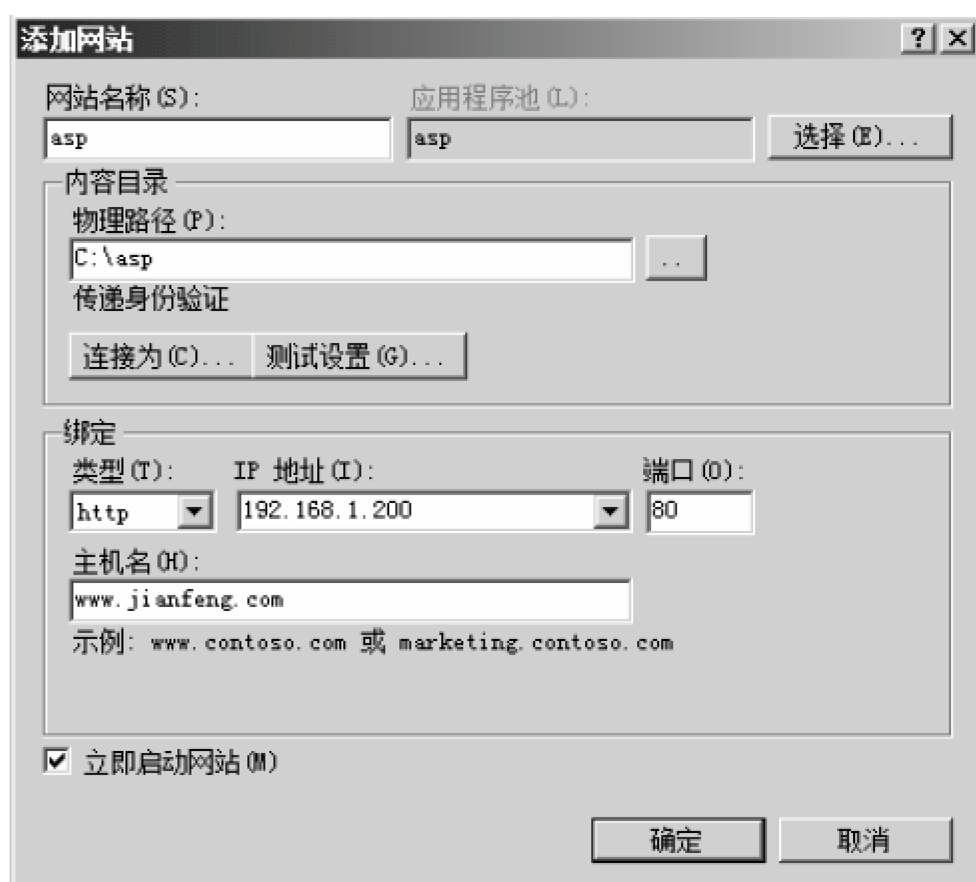


图 10-13 【添加网站】对话框



图 10-14 配置 asp 的默认文档

06 打开【默认文档】窗格，如图 10-15 所示，单击右侧【添加】按钮。

07 弹出【添加默认文档】对话框，在【名称】文本框中输入网站 asp 的主页名称，如图 10-16 所示，本实例为 Default.aspx，单击【确定】按钮。



图 10-15 【默认文档】窗格



图 10-16 【添加默认文档】对话框

08 返回至【默认文档】窗格，如图 10-17 所示，右击左侧 asp 选项，在弹出的快捷菜单中选择【管理网站】➢【浏览】命令。

09 如图 10-18 所示，打开网站 asp。





图 10-17 asp 选项菜单

图 10-18 asp 网站

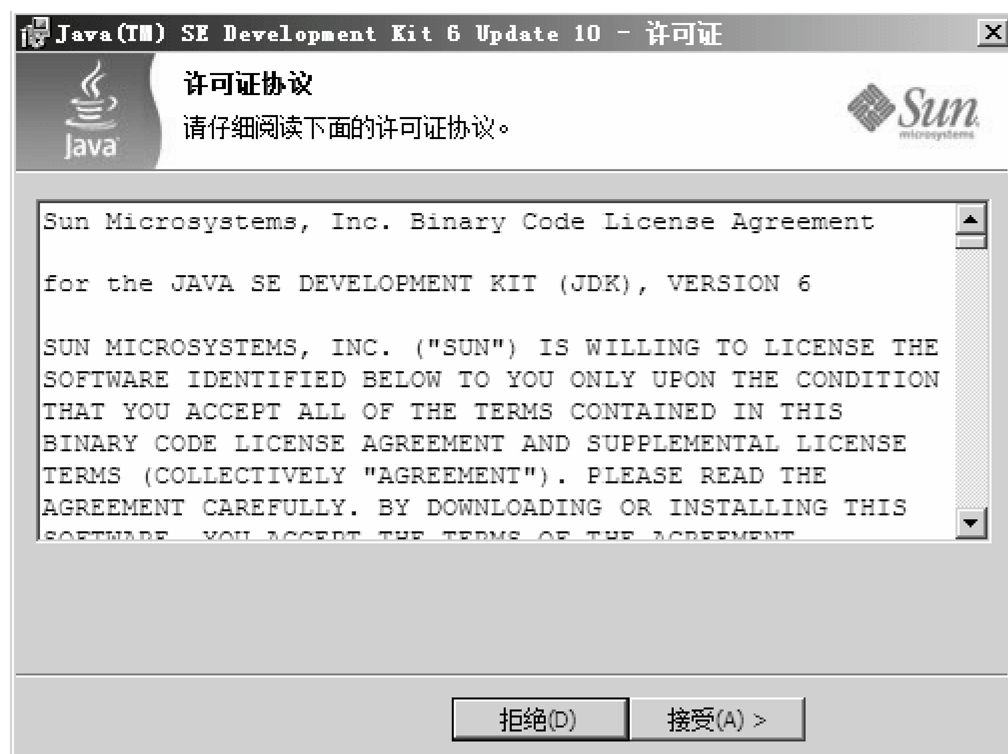
10.2 发布 JSP 动态网站

JSP 动态网站在制作大型商业网站方面具有独特的优势和稳定安全的特点，但是 JSP 动态网站的发布较为复杂。下面详细讲解使用 IIS 发布 JSP 动态网站的具体操作步骤。

10.2.1 安装 JDK 并配置环境变量

01 双击 JDK1.6 安装文件，弹出【许可证协议】对话框，单击【接受】按钮，如图 10-19 所示。

02 弹出【自定义安装】对话框，单击【更改】按钮，浏览选择 JDK 安装的物理路径，如图 10-20 所示，本实例采用默认安装路径 “C:\Program Files\Java\jdk1.6.0_10”，单击【下一步】按钮。



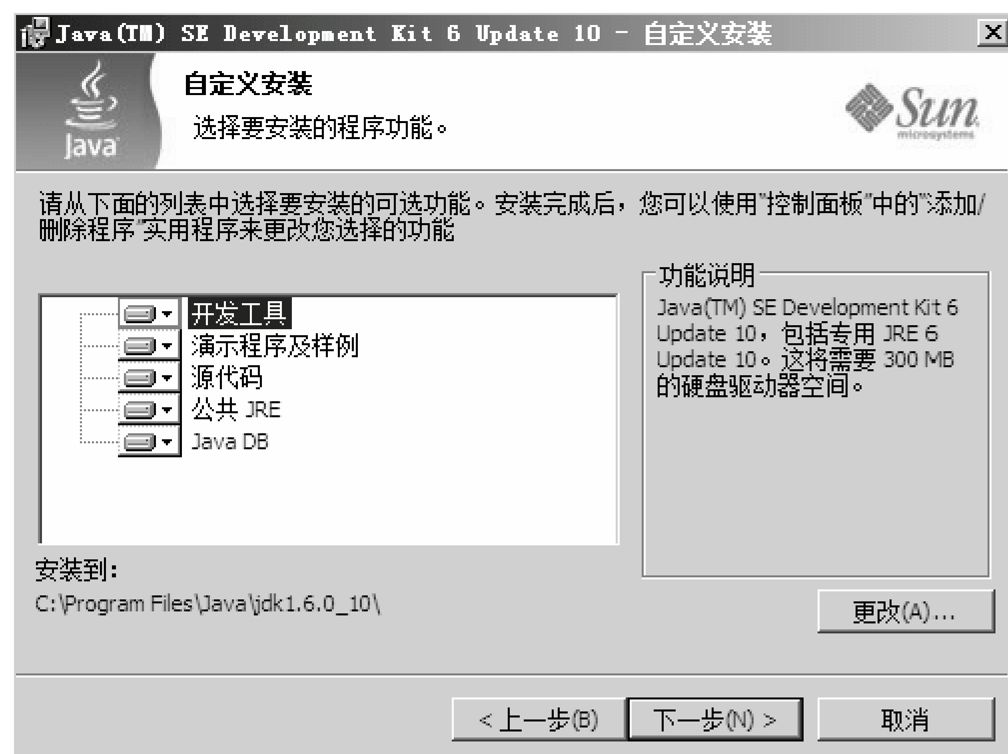


图 10-19 【许可证】对话框

图 10-20 【自定义安装】对话框

03 弹出【正在安装】对话框，如图 10-21 所示，显示 JDK 的安装进度，并显示安装进度条。

04 弹出【目标文件夹】对话框，单击【更改】按钮选择 jre6 安装的物理路径，如图 10-22 所示，本实例采用默认值 “C:\Program Files\Java\jre6”，单击【下一步】按钮。



图 10-21　【正在安装】对话框



图 10-22　【目标文件夹】对话框

05 弹出【正在安装 Java】对话框，如图 10-23 所示，显示 Java 安装进度，并显示安装进度条。

06 弹出安装完成对话框，如图 10-24 所示，单击【完成】按钮。



图 10-23　【正在安装 Java】对话框



图 10-24　安装完成对话框

07 更改环境变量。右击系统桌面上的【计算机】图标，如图 10-25 所示，在弹出的快捷菜单中选择【属性】命令。

08 弹出【系统】窗口，如图 10-26 所示，选择左侧【高级系统设置】选项。



图 10-25　右击【计算机】图标



图 10-26　【系统】窗口

09 弹出【系统属性】对话框，如图 10-27 所示，单击【环境变量】对话框。

10 弹出【环境变量】对话框，如图 10-28 所示，单击【系统变量】选项域的【新建】按钮。

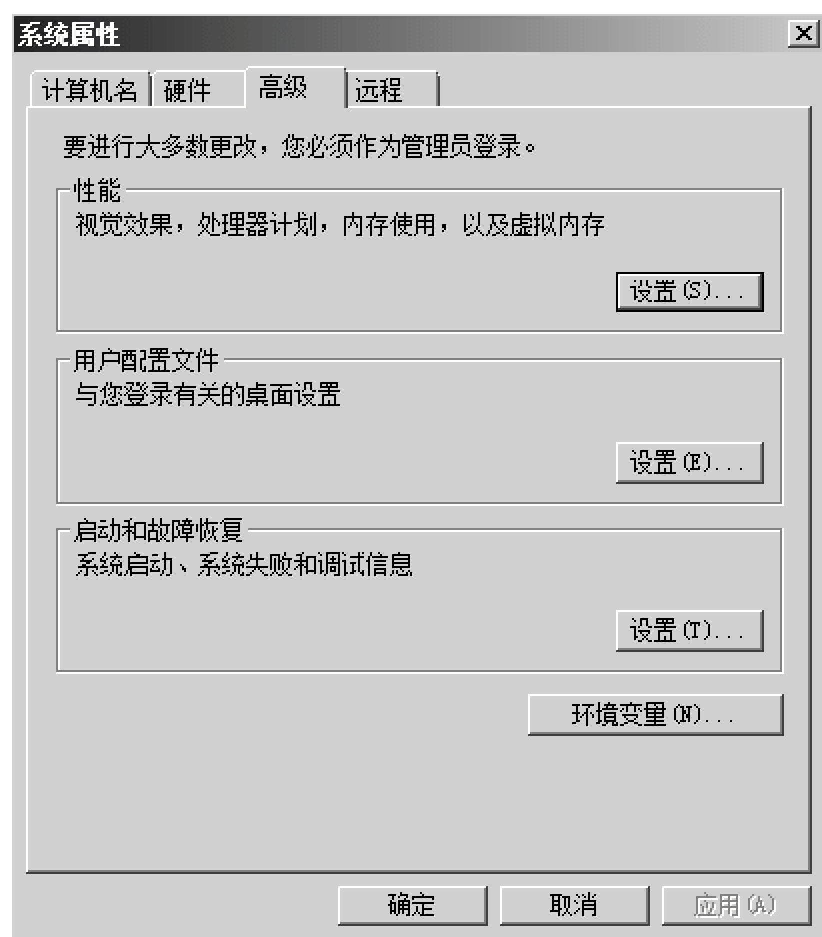


图 10-27 【系统属性】对话框



图 10-28 【环境变量】对话框

11 弹出【新建系统变量】对话框，如图 10-29 所示，在【变量名】文本框中输入变量名为“JAVA_HOME”，在【变量值】文本框中输入变量值为“C:\Program Files\Java\jdk1.6.0_10”，单击【确定】按钮。

12 返回至【环境变量】对话框，如图 10-30 所示，单击【系统变量】选项域的【新建】按钮。



图 10-29 【新建系统变量】对话框 1



图 10-30 【环境变量】对话框 1

13 弹出【新建系统变量】对话框，如图 10-31 所示，在【变量名】文本框中输入变量名为“classpath”，在【变量值】文本框中输入变量值为“.;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar;”，单击【确定】按钮。

14 返回至【环境变量】对话框，如图 10-32 所示，选择【系统变量】选项域的 Path 变量值，然后单击【编辑】按钮。

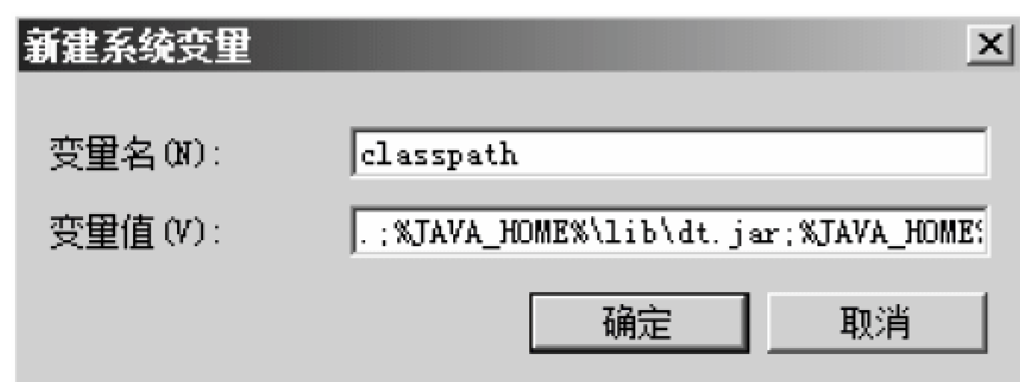


图 10-31 【新建系统变量】对话框 2

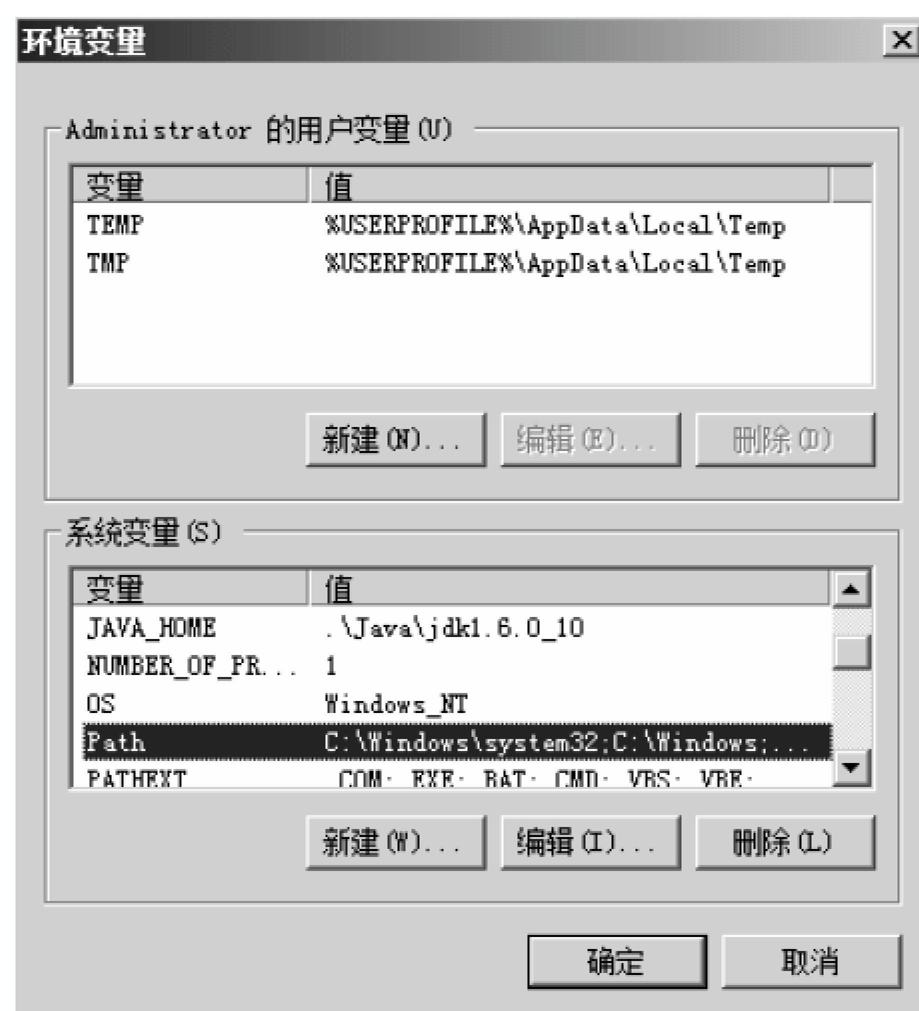


图 10-32 【环境变量】对话框 2

15 弹出【编辑系统变量】对话框，如图 10-33 所示，在【变量值】文本框后面添加变量值“;%JAVA_HOME%\bin”，单击【确定】按钮。

16 返回至【环境变量】对话框，如图 10-34 所示，单击【确定】按钮。



图 10-33 【编辑系统变量】对话框

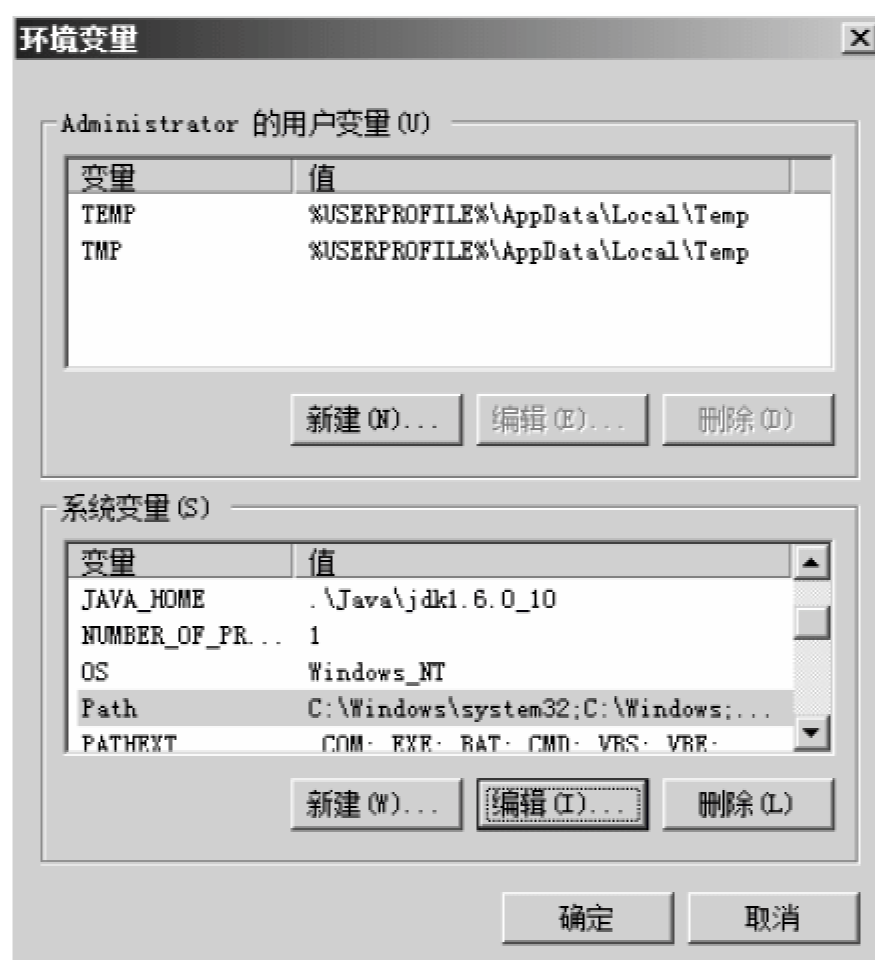


图 10-34 【环境变量】对话框 3

17 测试 Java 环境。打开记事本，在里面输入如下代码，保存在系统桌面上，并且命名为“Test.java”。

```
public class Test{
public static void main(String args[]){
System.out.println("Test success");
}
}
```

18 选择【开始】➢【运行】选项，弹出【运行】对话框，在【打开】文本框中输入“cmd”，单击【确定】按钮，如图 10-35 所示。

19 弹出 cmd 窗口，使用“cd”命令切换至“Test.Java”测试文件所在的目录，本实例测试文件所在的目录为系统桌面，如图 10-36 所示，所示输入命令“Javac Test.java”，按 Enter 键。如果没有报错，输入命令“java Test”，按 Enter 键，输入为“Test success”，则环境变量配置成功。

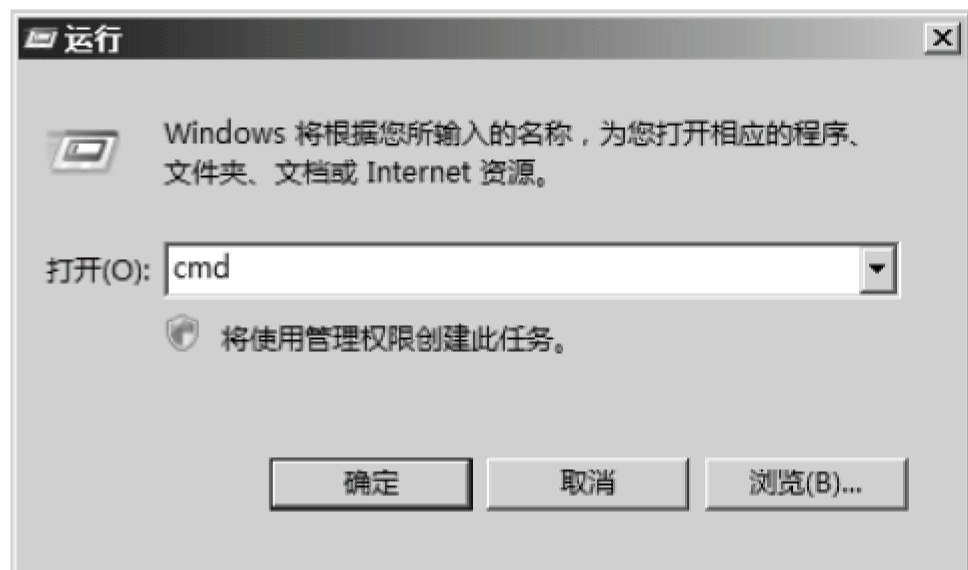


图 10-35 【运行】对话框

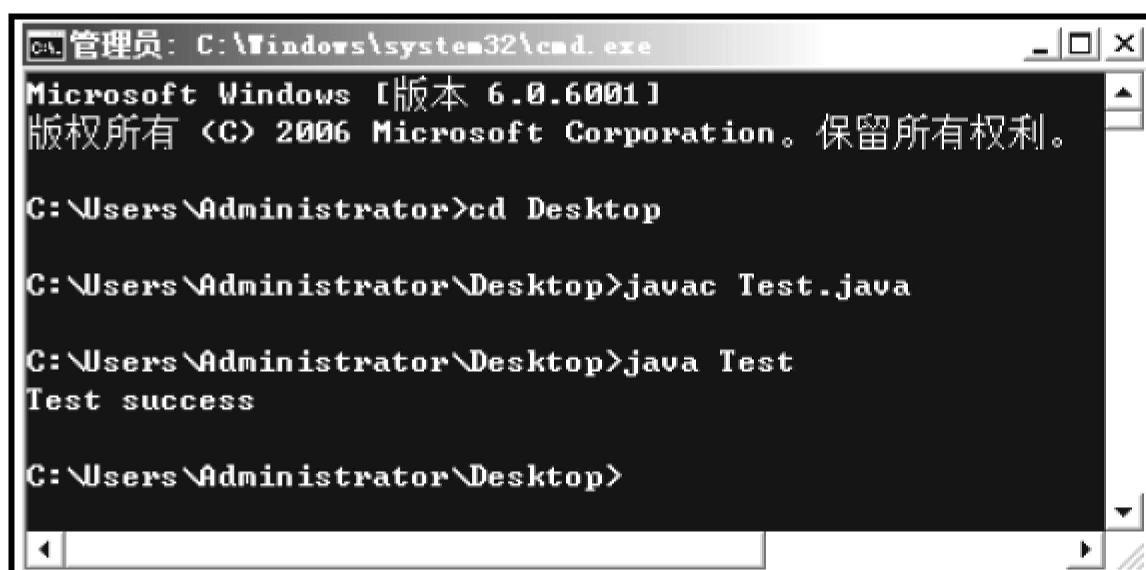


图 10-36 cmd 窗口

10.2.2 安装 Tomcat 并配置环境变量

Tomcat 是 Apache 基金会下的一款支持 JSP 环境的开源软件，安装 Tomcat 软件的具体操作步骤如下。

01 双击 Tomcat 安装文件，弹出 Tomcat 安装对话框，如图 10-37 所示，单击 Next 按钮。

02 弹出 License Agreement 对话框，如图 10-38 所示，单击 I Agree 按钮。



图 10-37 Tomcat 安装对话框

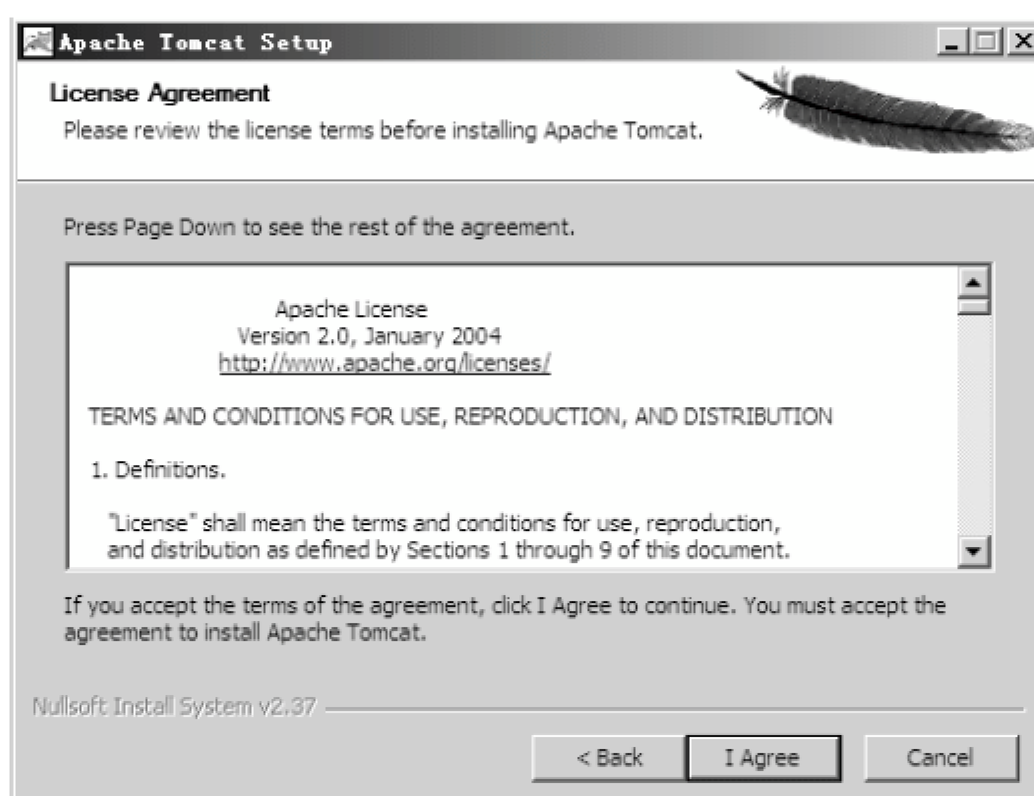


图 10-38 License Agreement

03 弹出 Choose Components 对话框，如图 10-39 所示，单击 Next 按钮。

04 弹出 Choose Install Location 对话框，单击 Browse 按钮，更改 Tomcat 安装路径，如图 10-40 所示，本实例采用默认安装路径“C:\Program Files\Apache Software Foundation\Tomcat 6.0”，单击 Next 按钮。

05 弹出 Configuration 对话框，如图 10-41 所示，在 HTTP/1.1 Connector Port 文本框中输入端口号“8080”，单击 Next 按钮。

06 弹出 Java Virtual Machine 对话框，如图 10-42 所示，单击 ... 按钮。

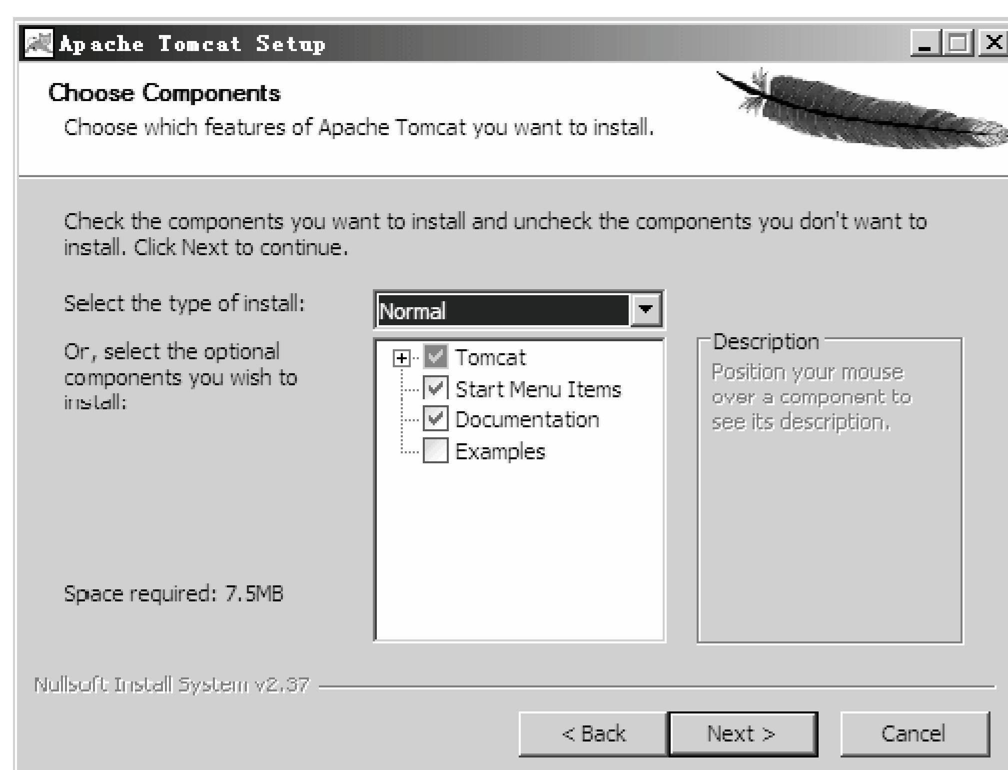


图 10-39　Choose Components 对话框

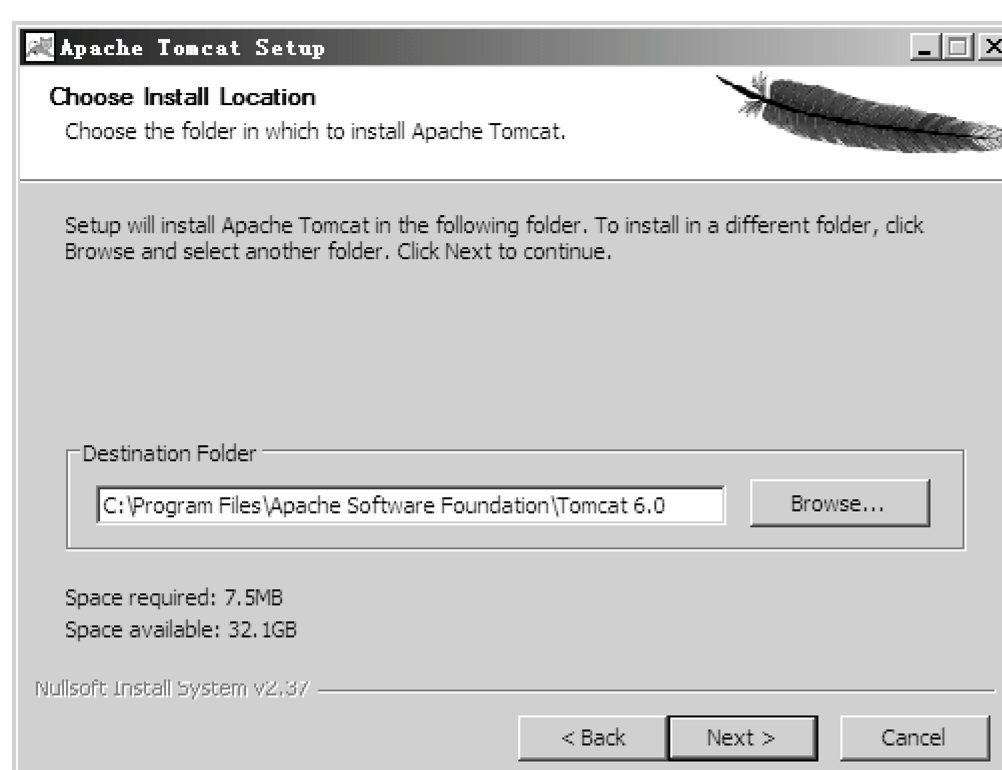


图 10-40　Choose Install Location 对话框

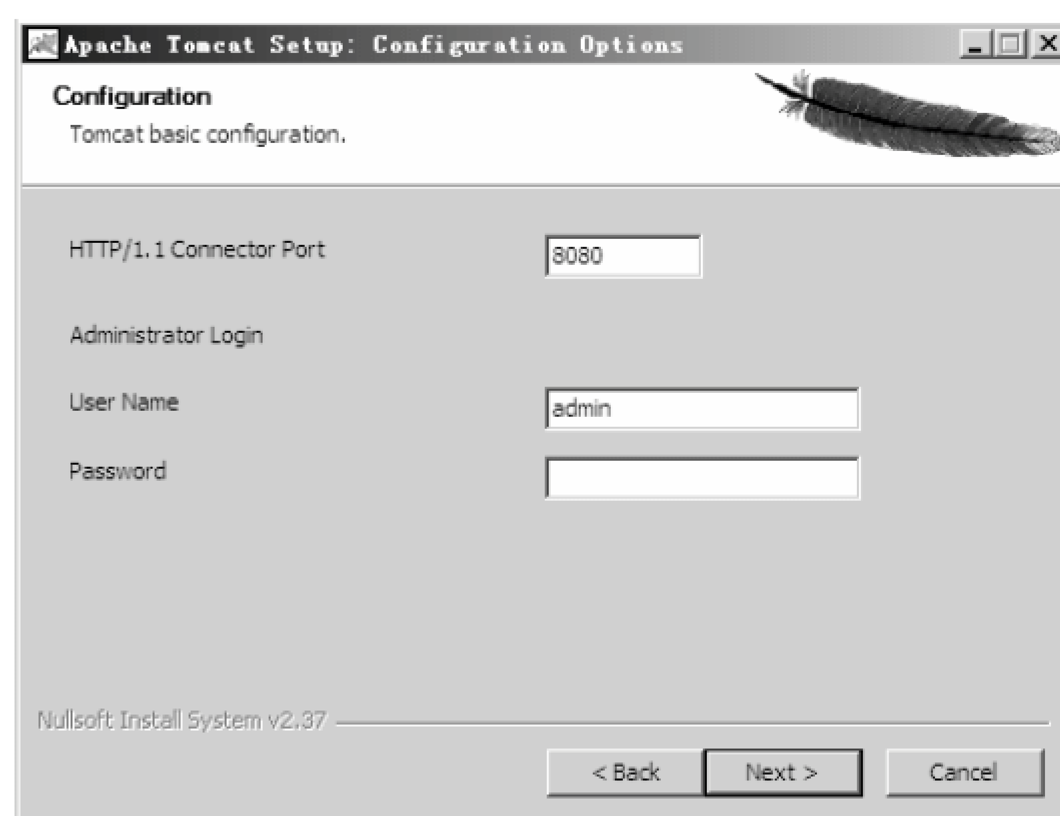


图 10-41　Configuration 对话框

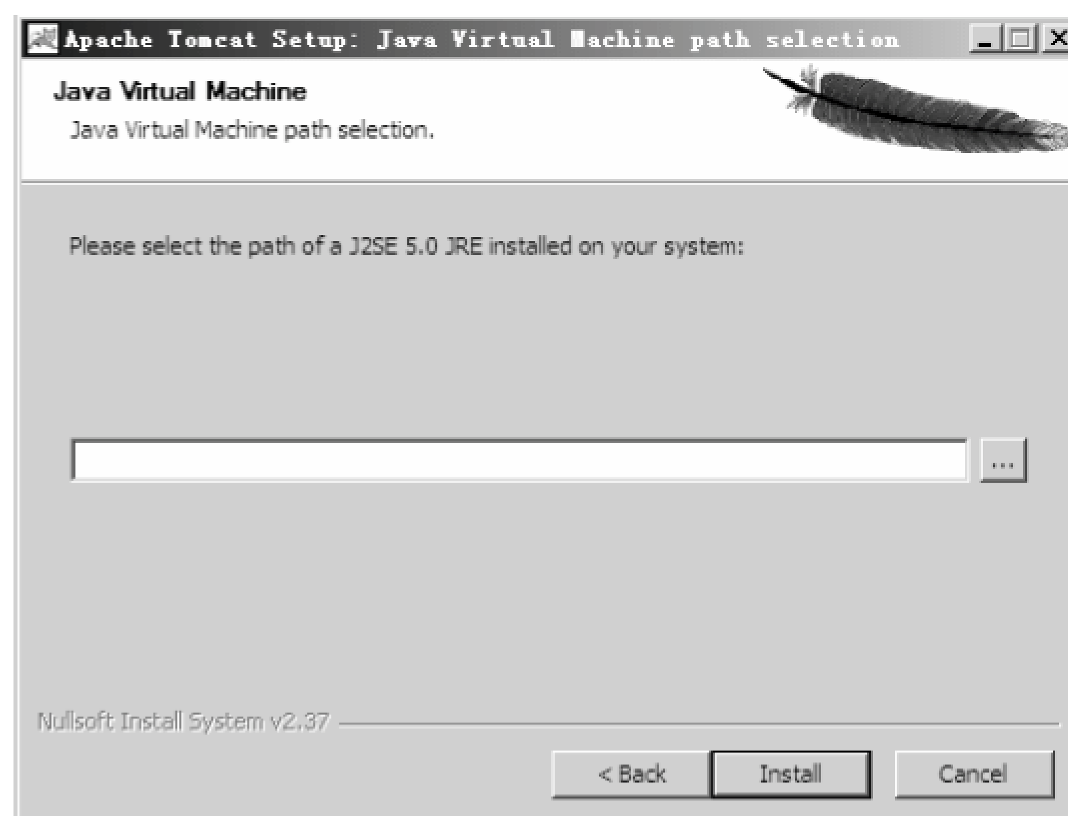


图 10-42　Java Virtual Machine 对话框

07　弹出【浏览文件夹】对话框，浏览找到 JDK 的安装路径，如图 10-43 所示，本实例为“C:\program File\Java\jdk1.6.0_10\jre”，单击【确定】按钮。

08　返回至 Java Virtual Machine 对话框，如图 10-44 所示，单击 Install 按钮。



图 10-43　【浏览文件夹】对话框

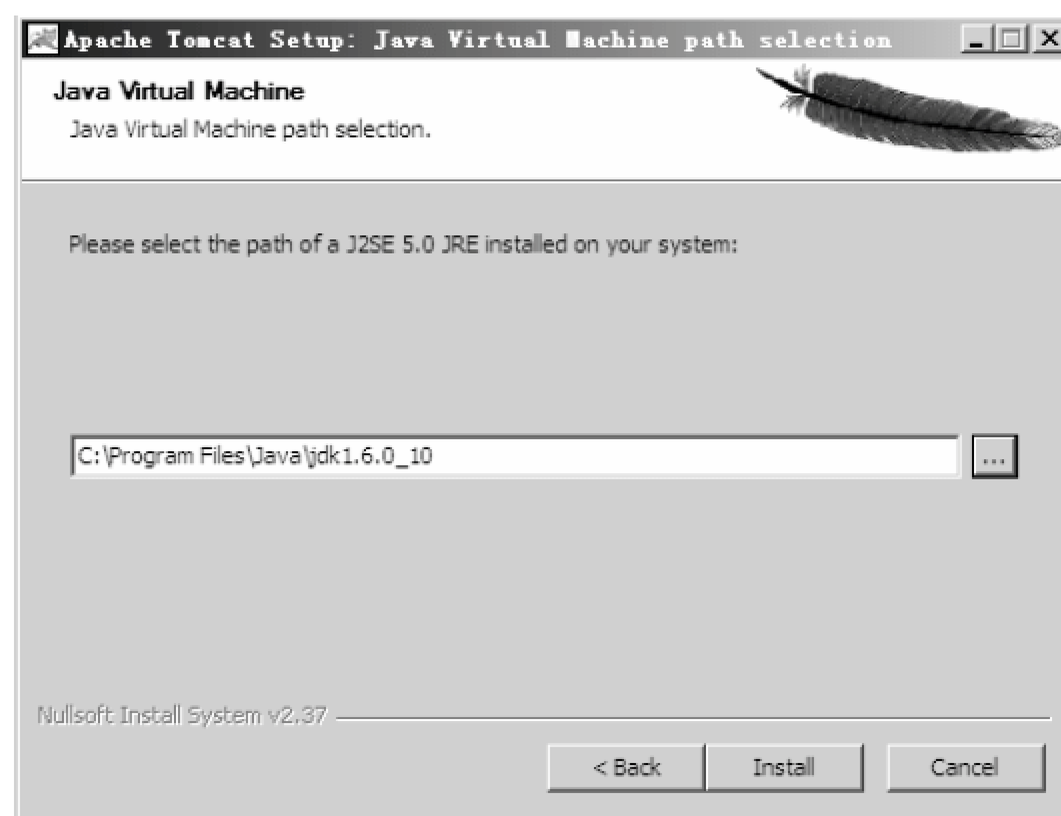


图 10-44　Java Virtual Machine 对话框

09　弹出 Installing 对话框，如图 10-45 所示，显示 Tomcat 的安装进度。

10　弹出 Completing the Apache Tomcat Setup Wizard 对话框，如图 10-46 所示，单击 Finish

按钮。

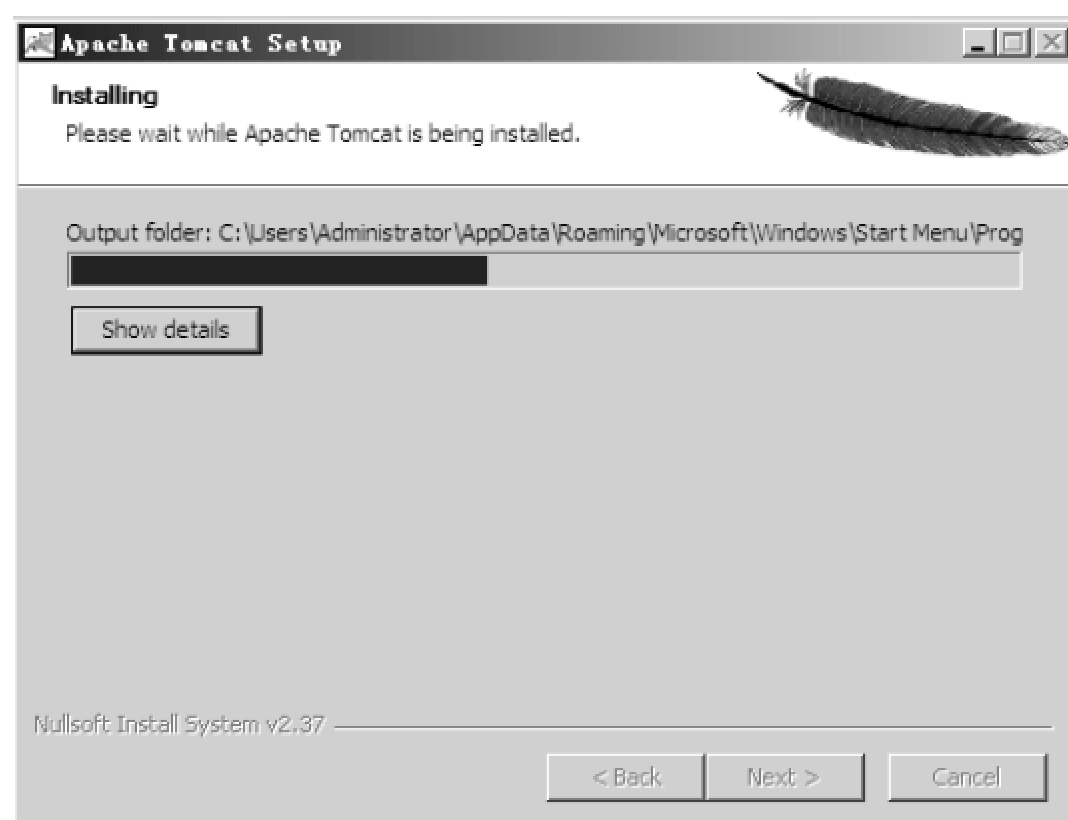


图 10-45　Installing 对话框



图 10-46　Tomcat Setup Wizard 对话框

11 更改环境变量。右击系统桌面上的【计算机】图标，在弹出的快捷菜单中选择【属性】命令。

12 弹出【系统】窗口，选择左侧【高级系统设置】选项。

13 弹出【系统属性】对话框，单击【环境变量】按钮。

14 弹出【环境变量】对话框，单击【系统变量】选项域的【新建】按钮。

15 弹出【新建系统变量】对话框，在【变量名】文本框中输入变量名为“CATALINA_HOME”，在【变量值】文本框中输入变量值为“C:\Program Files\Apache Software Foundation\Tomcat 6.0”，如图 10-47 所示，单击【确定】按钮。

16 返回至【环境变量】对话框，如图 10-48 所示，单击【系统变量】选项域的【新建】按钮。



图 10-47　【新建系统变量】对话框



图 10-48　【环境变量】对话框

17 弹出【新建系统变量】对话框，在【变量名】文本框中输入变量名为“CATALINA_BASE”，在【变量值】文本框中输入变量值为“C:\Program Files\Apache Software Foundation\Tomcat 6.0”，如图 10-49 所示，单击【确定】按钮。

18 返回至【环境变量】对话框，如图 10-50 所示，单击【系统变量】选项域的【新建】按钮。



图 10-49 【新建系统变量】对话框

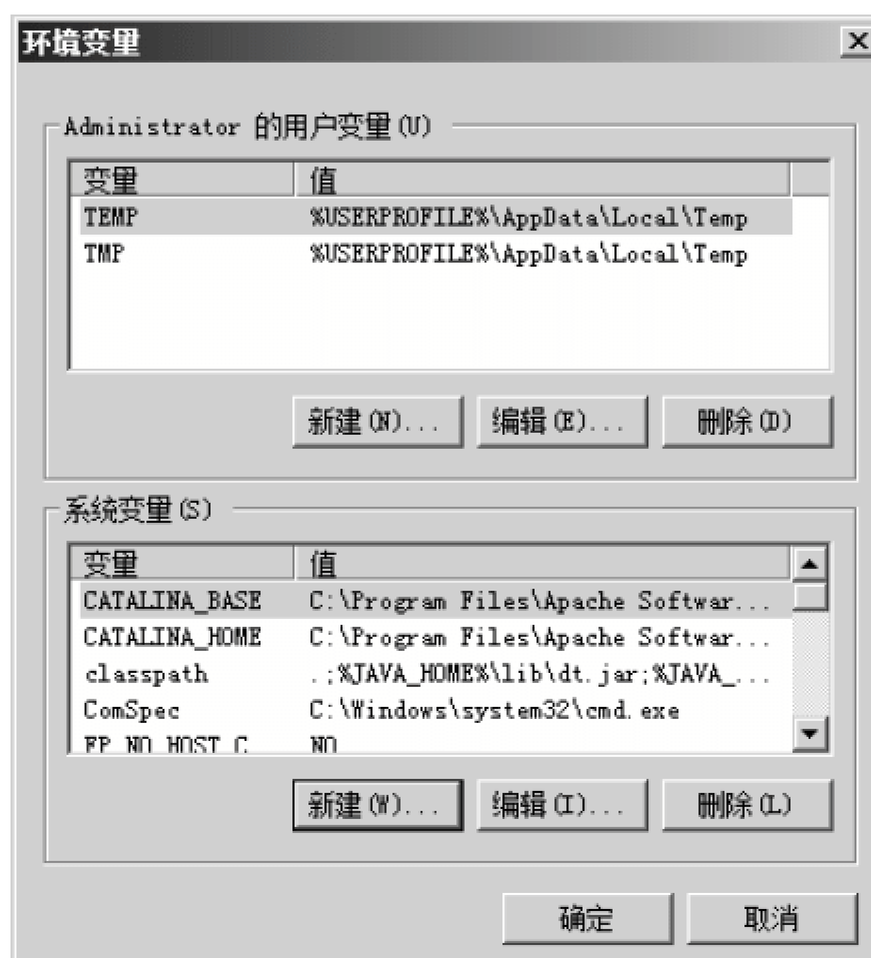


图 10-50 【环境变量】对话框

19 弹出【新建系统变量】对话框，在【变量名】文本框中输入变量名为“TOMCAT_HOME”，在【变量值】文本框中输入变量值为“C:\Program Files\Apache Software Foundation\Tomcat 6.0”，如图 10-51 所示，单击【确定】按钮。

20 返回至【环境变量】对话框，选中【系统变量】选项域的 classpath 一行，如图 10-52 所示，单击【编辑】按钮。



图 10-51 【新建系统变量】对话框

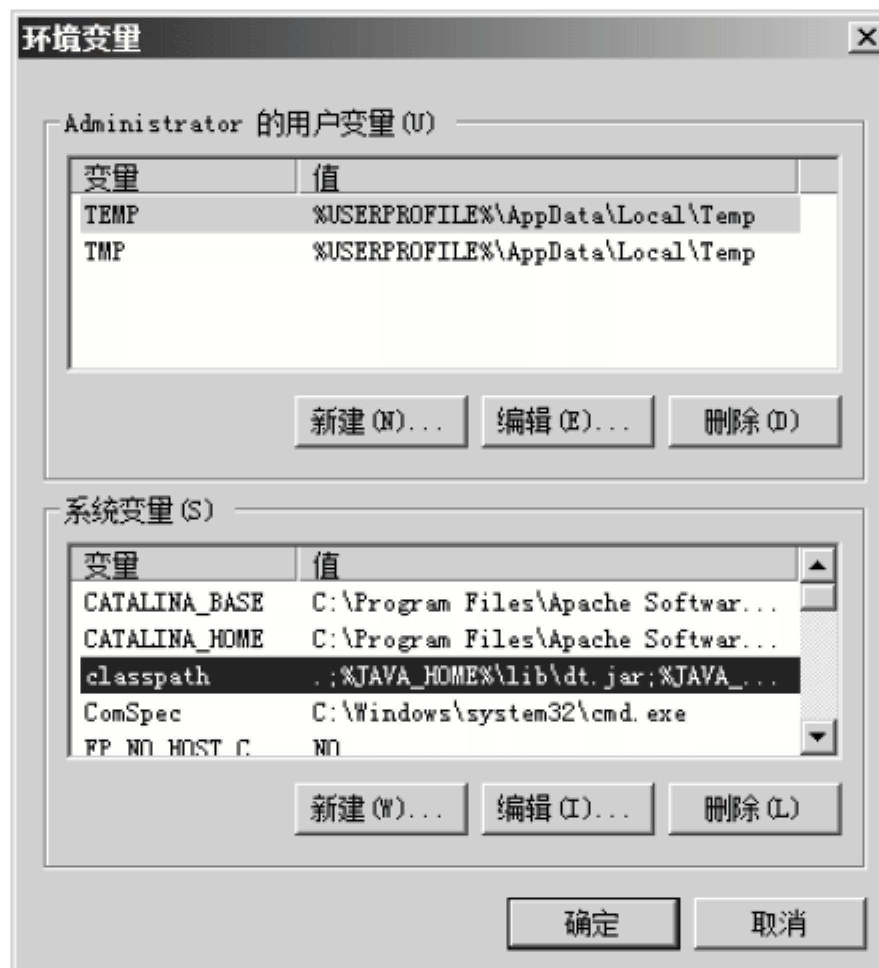


图 10-52 【环境变量】对话框

21 弹出【编辑系统变量】对话框，在【变量值】文本框中将变量值修改为“.;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar;%CATALINA_HOME%\lib\servlet-api.jar;”，如图 10-53 所示，单击【确定】按钮。

22 返回至【环境变量】对话框，如图 10-54 所示，单击【确定】按钮。

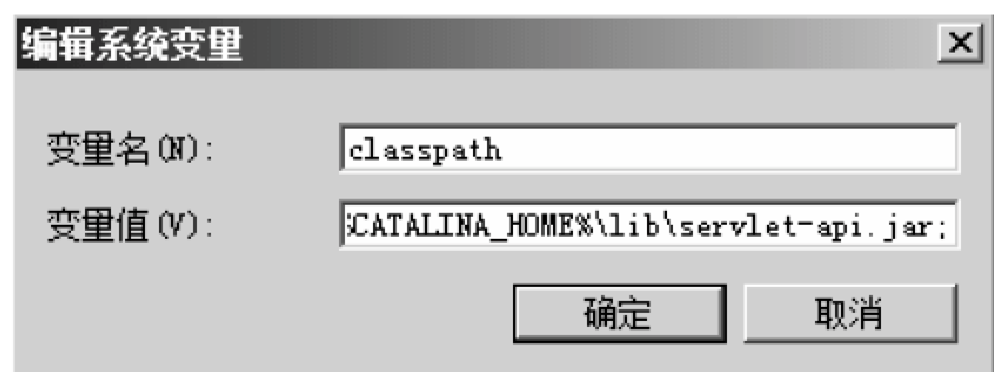


图 10-53 【编辑系统变量】对话框

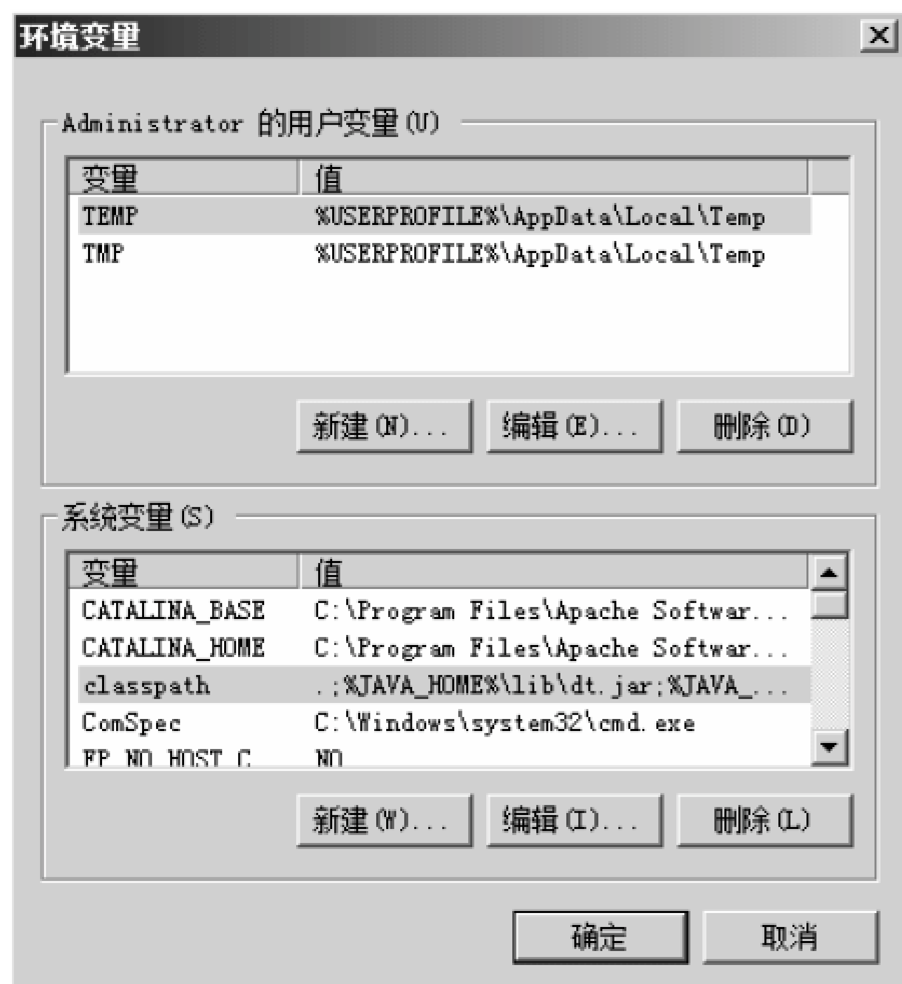


图 10-54 【环境变量】对话框

23 返回至【系统属性】对话框，单击【确定】按钮。

24 选择【开始】➢【所有程序】➢【Apache Tomcat 6.0】➢【Monitor Tomcat】命令，如图 10-55 所示，启动 Tomcat。



图 10-55 启动 Tomcat

25 打开 IE 浏览器，在地址栏里输入 http://127.0.0.1:8080，按 Enter 键，如图 10-56 所示，正确打开 Tomcat 欢迎界面，表示 Tomcat 安装成功。

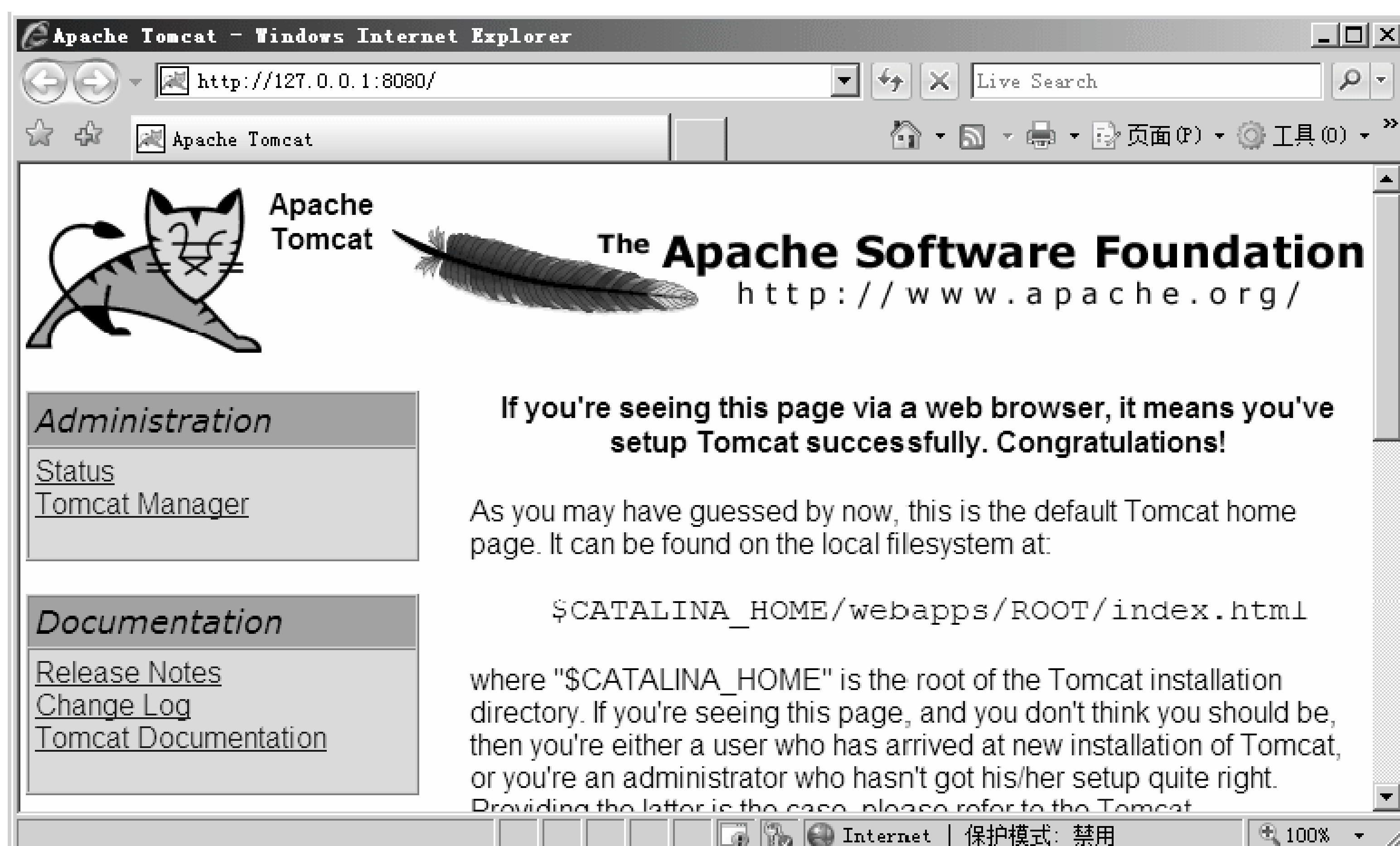


图 10-56　Tomcat 欢迎界面

10.2.3　检测 Tomcat 平台

下面来检查在 Tomcat 平台中运行 JSP 与 Servlet 程序是否成功，具体操作步骤如下。

01 首先检测 JSP，检查 Tomcat 的安装目录的 Web apps 目录，也就是物理路径为“C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps”的目录里可以看到 Root，examples，tomcat-docs 等 Tomcat 自带的目录。

02 在物理路径为“C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps”的目录下新建一个目录，命名为 myapp，在 myapp 下新建一个目录 WEB -INF，然后在 WEB -INF 目录新建一个文件 Web .xml，然后在 Web .xml 文件写入如下内容：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Web -app>
<display-name>My Web   Application</display-name>
<description>
A application for test.
</description>
</Web -app>
```

03 在上一步骤建立的 myapp 目录里新建一个 JSP 测试页面，命名为 index.jsp，写入内容如下：

```
<html><body><center>
Now time is: <%=new java.util.Date()%>
</center></body></html>
```

04 重启 Tomcat，右击桌面右下角 Tomcat 图标，在弹出的快捷菜单中选择 Stop service 命令，如图 10-57 所示，再选择 Sart service 命令。

05 打开 IE 浏览器，在地址栏输入 http://127.0.0.1:8080/myapp/index.jsp，按 Enter 键，可以

看到如图 10-58 所示界面，表明 JSP 正常。



图 10-57　重启 Tomcat

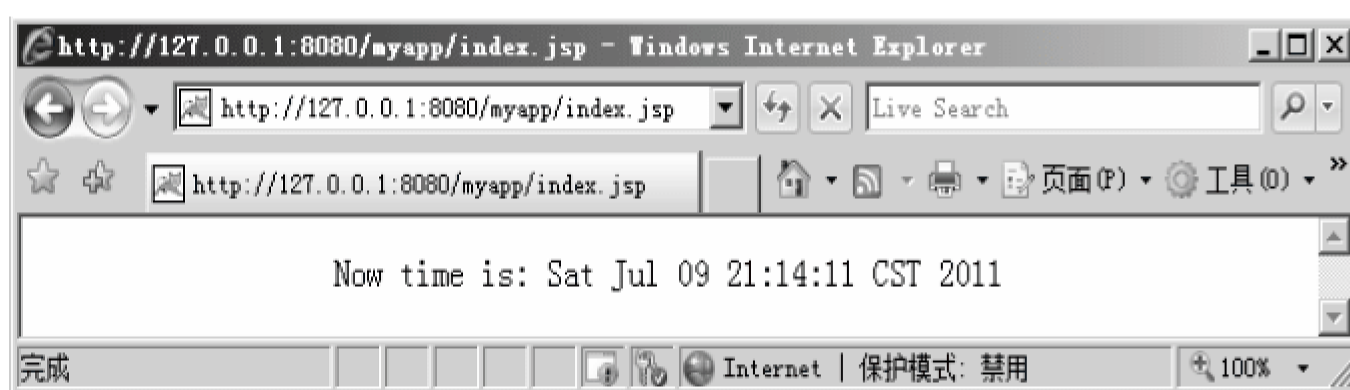


图 10-58　JSP 网站

06 测试 Servlet，在桌面上建立一个文本文档，命名为 HelloWorld.java，写入内容如下：

```
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;
public class HelloWorld extends HttpServlet
{
public void doGet(HttpServletRequest request,HttpServletResponse response)throws ServletException,IOException
{
response.setContentType("text/html");
PrintWriter out = response.getWriter();
out.println("<html><head><title>");
out.println("This is my first Servlet");
out.println("</title></head><body>");
out.println("<h1>Hello,World!</h1>");
out.println("</body></html>");
}
}
```

07 选择【开始】➢【运行】命令，弹出【运行】对话框，在【打开】文本框输入“cmd”，单击【确定】按钮。

08 弹出【命令提示符】对话框，使用“cd”命令切换至系统桌面，输入命令“javac HelloWorld.java”编译文件，按 Enter 键。如果出现如图 10-59 所示的错误，把 Tomcat 安装目录“C:\Program Files\Apache Software Foundation\Tomcat 6.0”下的 lib 里面的 servlet-api.jar 文件复制到 JDK 安装目录“C:\Program Files\Java\jdk1.6.0_10”下的 jre\lib\ext 中，再次输入命令“javac HelloWorld.java”编译文件，编译生成“HelloWorld.class”文件。



图 10-59　cmd 窗口

09 在“C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps \myapp\WEB -INF”

文件夹中，建立一个文件夹，命名为 classes，然后将上文编译生成的“HelloWorld.class”文件放入“classes”文件夹中。用记事本打开该目录下的 Web .xml 文件，修改成如下内容并保存。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Web -app>
<display-name>My Web    Application</display-name>
<description>
A application for test.
</description>
<servlet>
    <servlet-name>HelloWorld</servlet-name>
    <servlet-class>HelloWorld</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>HelloWorld</servlet-name>
    <url-pattern>/HelloWorld</url-pattern>
</servlet-mapping>
</Web -app>
```

10 重启 Tomcat，右击桌面右下角 Tomcat 图标，在弹出的快捷菜单中选择 Stop service 命令，然后选择 Start service 命令。

11 打开 IE 浏览器，在地址栏输入“http://127.0.0.1:8080/myapp/HelloWorld”，按 Enter 键，可以看到如图 10-60 所示的界面，表明 JSP 正常。

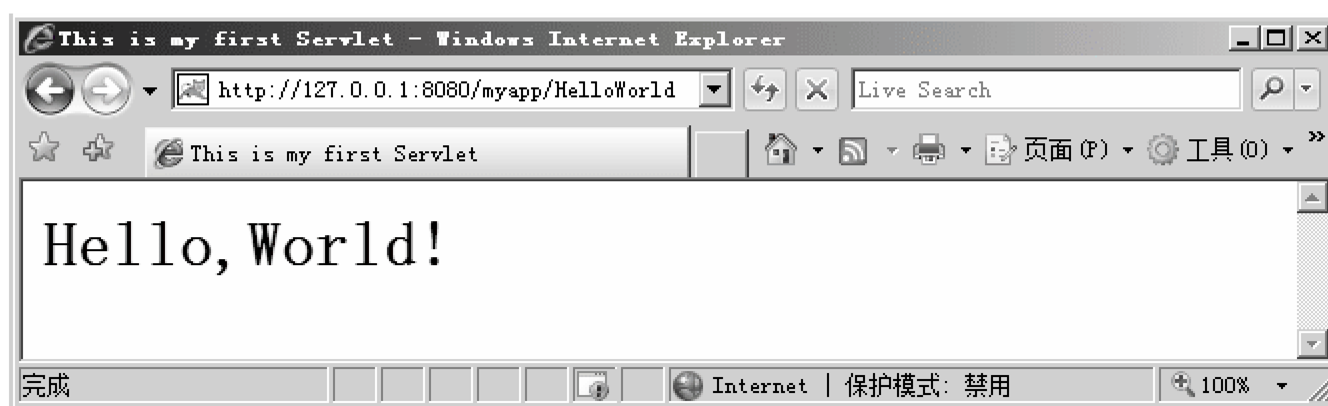


图 10-60　JSP 界面

10.2.4　用 JK 整合 IIS 6 与 Tomcat 6

Tomcat 安装完成后，就可以发布 JSP 动态网站，但是 Tomcat 的不可管理性会对后期的网站维护造成一定的困难，这时需要使用 JK 文件将 IIS 6 和 Tomcat 连接起来，利用 IIS 来管理 Tomcat 发布的动态 JSP 网站，用 JK 文件整合 IIS 6 和 Tomcat 6 的详细操作步骤如下。

01 首先在“C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf”文件夹中新建两个文件，并分别命名为“workers.properties”和“uriworkermap.properties”。其中修改文件“workers.properties”内容如下：

```
workers.tomcat  home=C:\Program Files\Apache Software Foundation\Tomcat 6.0\
workers.java  home=C:\Program Files\Java\jdk1.6.0  10\
ps=\
worker.list=ajp13
worker.ajp13.port=8009
worker.ajp13.host=localhost
```

```
worker.ajp13.type=ajp13
worker.ajp13.lbfactor=1
修改文件“uriworkermap.properties”内容如下：
/*.jsp=ajp13
/*.do=ajp13
!/*.jpg=ajp13
!/*.gif=ajp13
!/*.bmp=ajp13
```

02 在系统桌面上，建立一个文本文档并将其命名为“isapi_redirect.reg”，如果 Tomcat 安装目录物理路径是“C:\Program Files\Apache Software Foundation\Tomcat 6.0”，JK 文件名为“isapi_redirect.dll”，则将文件“isapi_redirect reg”文件内容修改如下：

```
Windows Registry Editor Version 5.00
[HKEY  LOCAL  MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0]
"log  file"="C:\Program Files\\Apache Software Foundation\Tomcat 6.0\logs\isapi.log"
"log_level"="debug"
"worker  file"="C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf\workers.properties"
"worker  mount  file"="C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf\uriworkermap.properties"
"extension_uri"="/jakarta/isapi_redirect.dll"
```

03 双击上一步骤制作的“isapi_redirect.reg”文件，如图 10-61 所示，弹出【注册表编辑器】提示框，提示将注册资料导入注册表，单击【是】按钮。

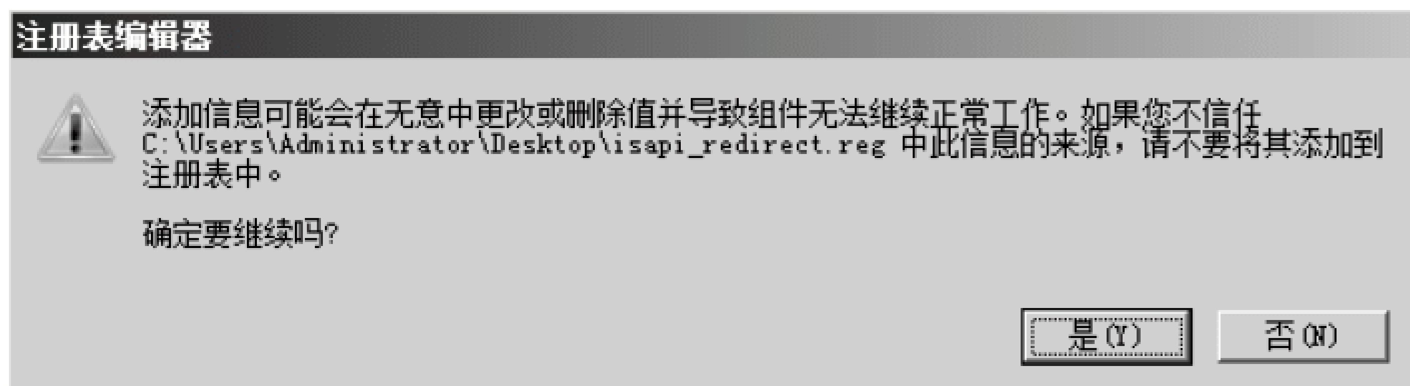


图 10-61　【注册表编辑器】提示框

04 弹出如图 10-62 所示的提示框表示导入注册表成功，单击【确定】按钮。



图 10-62　导入注册表成功

05 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，弹出【Internet 信息服务（IIS）管理器】窗口，如图 10-63 所示，选择左侧 WIN-013D26R8BJX 选项，双击【ISAPI 和 CGI 限制】图标。

06 弹出【ISAPI 和 CGI 限制】窗格，如图 10-64 所示，选择右侧【添加】选项。



图 10-63 【Internet 信息服务（IIS）管理器】窗口

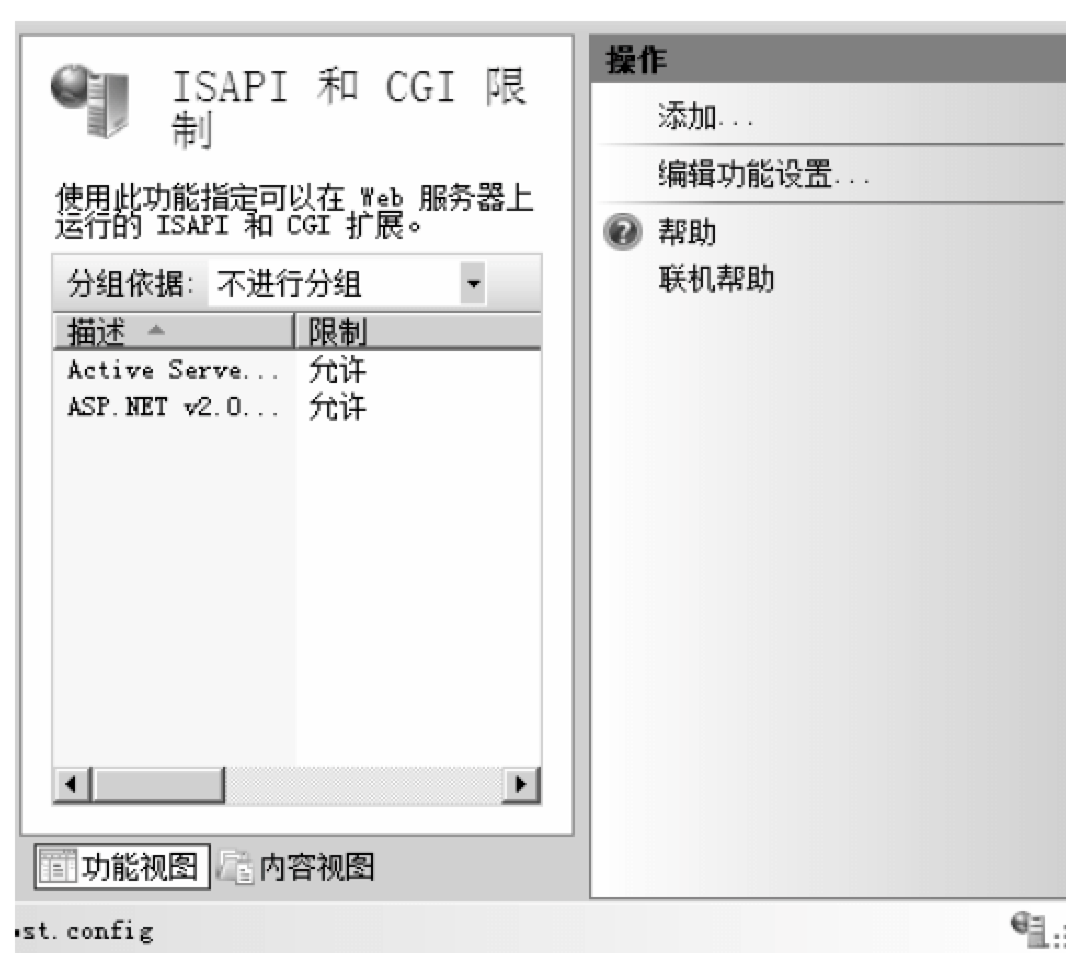


图 10-64 【ISAPI 和 CGI 限制】窗格

07 弹出【添加 ISAPI 或 CGI 限制】对话框，如图 10-65 所示，单击【ISAPI 或 CGI 路径】文本框后面的 .. 按钮。

08 弹出【打开】对话框，浏览找到本地的 JK 文件所在的目录，如图 10-66 所示，本实例 JK 文件所在的目录的物理路径为“C:\Users\Administrator\Desktop”，单击【打开】按钮。

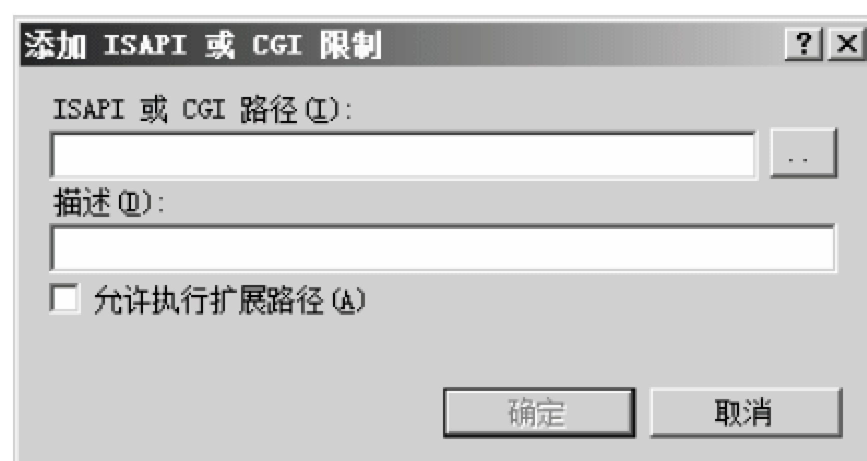


图 10-65 【添加 ISAPI 或 CGI 限制】对话框

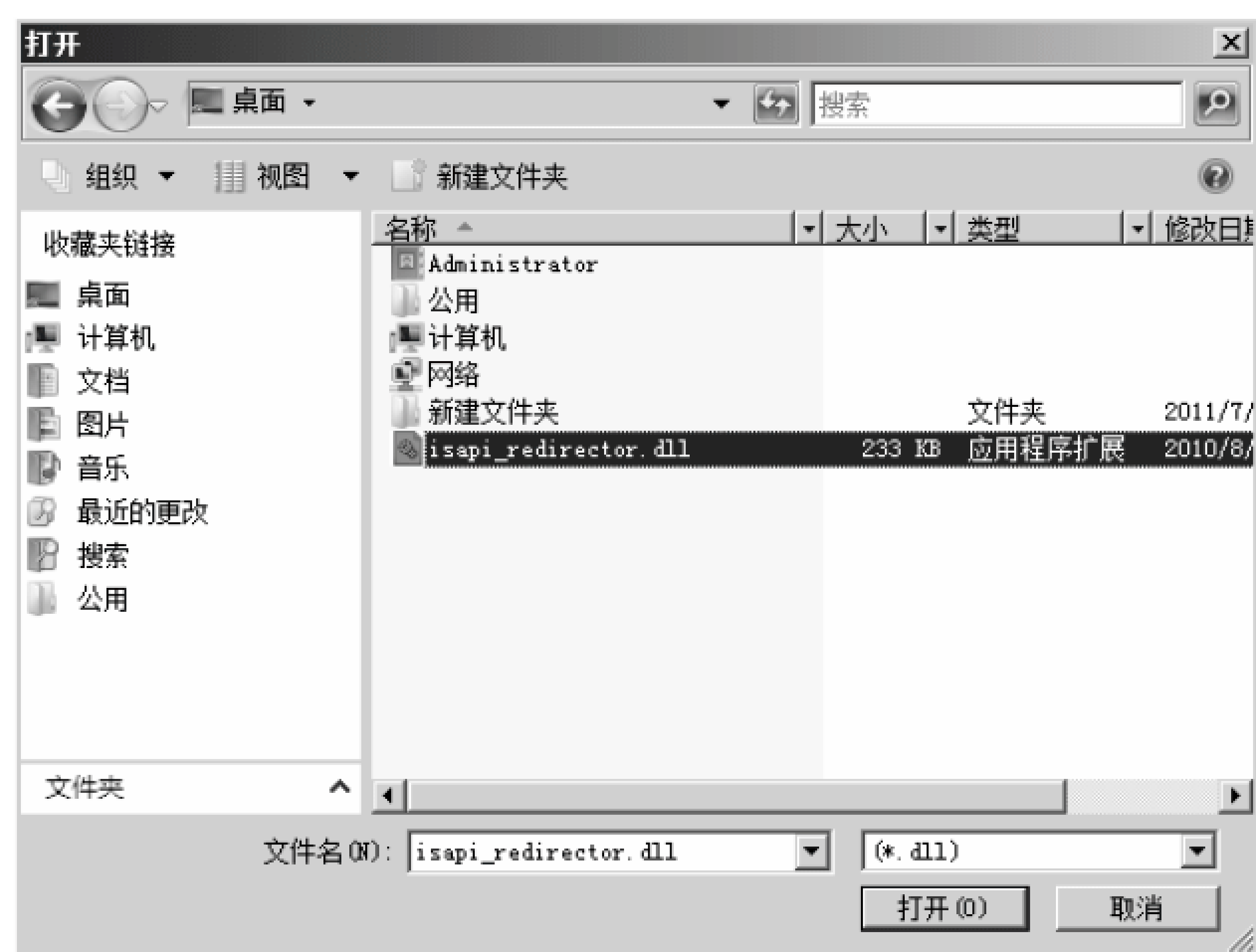


图 10-66 【打开】对话框

09 返回至【添加 ISAPI 或 CGI 限制】对话框，在【描述】文本框中输入“连接 Tomcat”，选中【允许执行扩展路径】复选框，单击【确定】按钮。

10 返回至【Internet 信息服务（IIS）管理器】窗口，选择左侧【网站】➢【默认站点】选项，双击【默认站点主页】窗格下的【ISAPI 筛选器】图标。

11 打开【ISAPI 筛选器】窗格，如图 10-67 所示，选择右侧【添加】选项。

12 弹出【添加 ISAPI 筛选器】对话框，在【筛选器名称】文本框中输入“jakarta”，在【可执行文件】文本框中输入 JK 文件“isapi_redirector.dll”的物理绝对路径，如图 10-68 所示，本实例为“C: \Users\Administrator\Desktop\isapi_redirector.dll”，单击【确定】按钮。

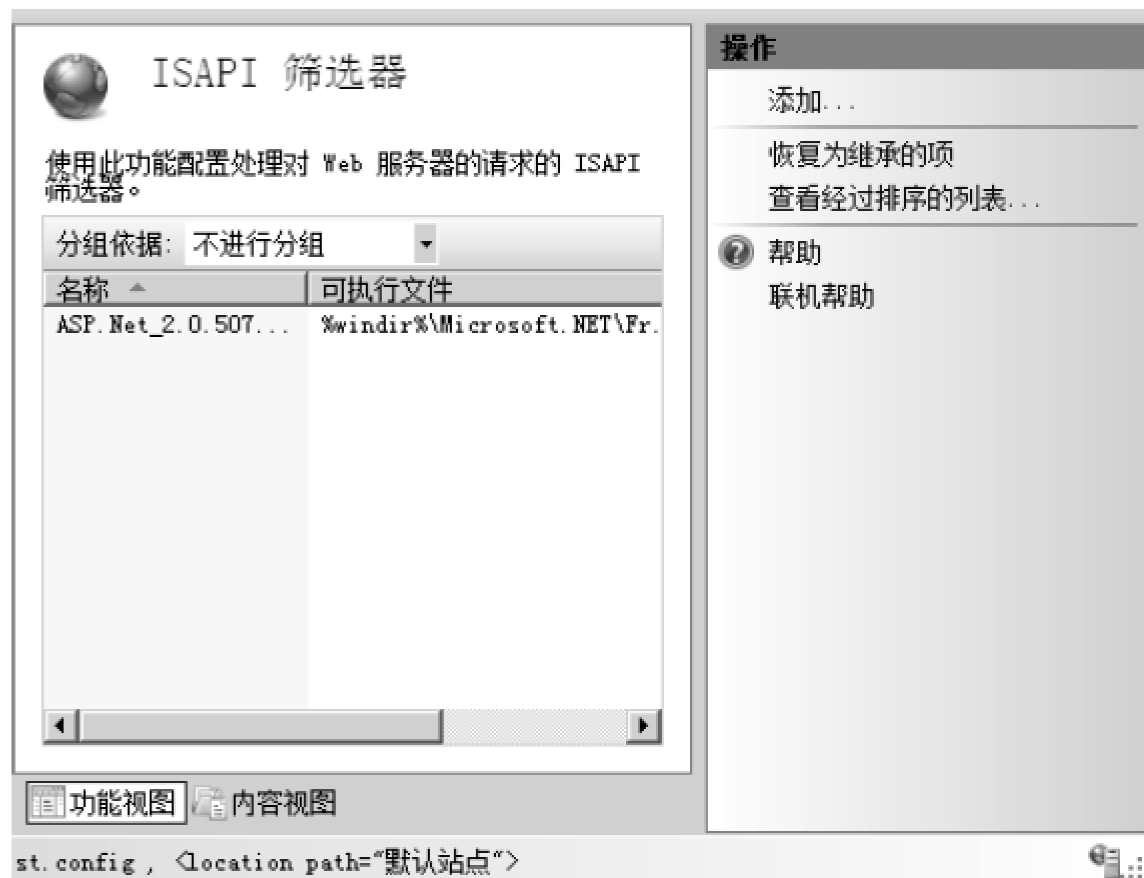


图 10-67 【ISAPI 筛选器】窗格



图 10-68 【添加 ISAPI 筛选器】对话框

13 返回至【Internet 信息服务（IIS）管理器】窗口，右击左侧【默认站点】选项，在弹出的快捷菜单中选择【管理网站】➢【高级设置】命令。

14 弹出【高级设置】对话框，单击【物理路径】文本框后面的...按钮。

15 弹出【浏览文件夹】对话框，浏览找到要发布的 JSP 网站所在文件夹。本实例选择上文中检测 JSP 时建立的“myapp”文件夹作为 JSP 网站的主目录，文件夹“myapp”文件夹的物理路径为“C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps\myapp”，单击【确定】按钮。

16 返回至【高级设置】对话框，单击【确定】按钮。

17 返回至【Internet 信息服务（IIS）管理器】窗口，双击【默认站点主页】窗格下的【处理程序映射】图标。

18 打开【处理程序映射】窗格，如图 10-69 所示，选择右侧【添加脚本映射】选项。

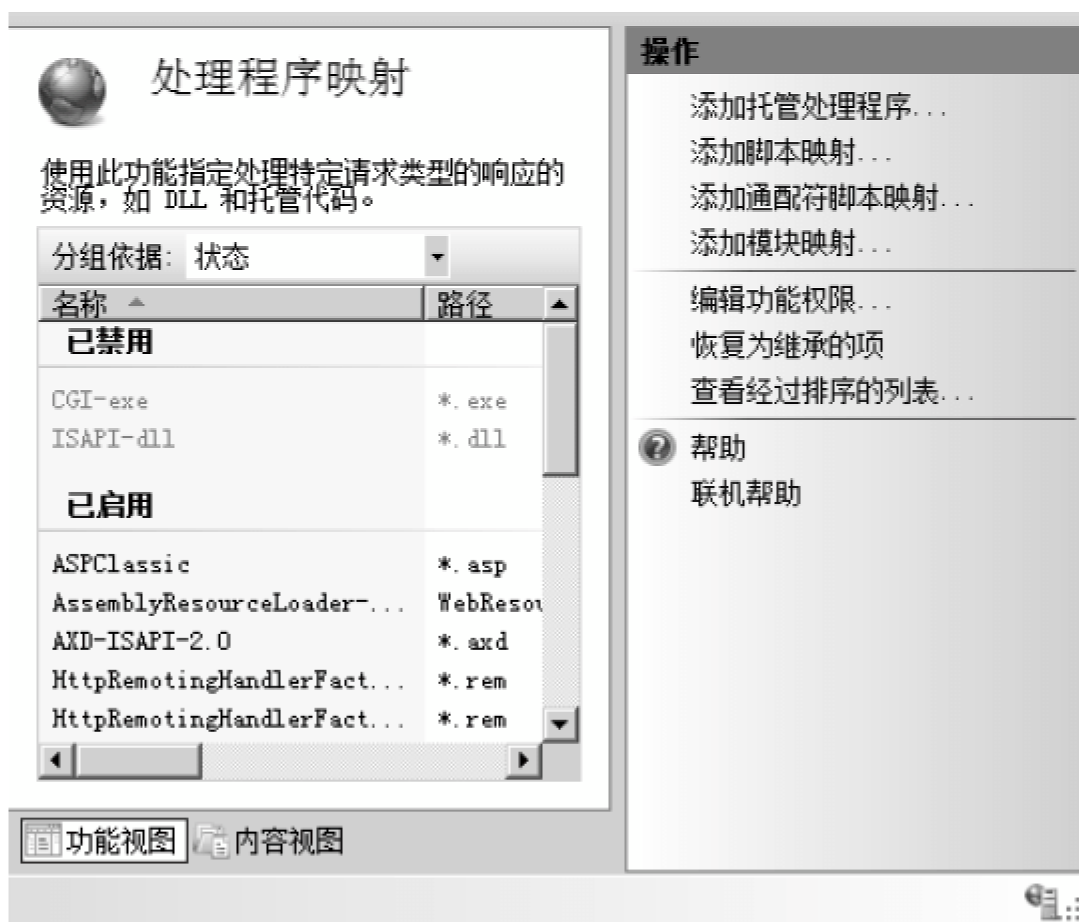


图 10-69 【处理程序映射】窗格

19 弹出【添加脚本映射】对话框，在【请求路径】文本框中输入“*.jsp”，如图 10-70 所示，单击【可执行文件】文本框后面的..图标。

20 弹出【打开】对话框，浏览找到 JK 文件，本实例 JK 文件物理路径为

“C:\Users\Administrator\Desktop\isapi_redirector.dll”，单击【打开】按钮。



图 10-70 【添加脚本映射】对话框

21 返回至【添加脚本映射】对话框，该对话框的主要功能是使得 IIS 可以自动识别 JSP 类型文件，在【名称】文本框中输入“JSP”，单击【确定】按钮。

22 弹出【添加脚本映射】提示框，如图 10-71 所示，单击【是】按钮，表示同意添加此 ISAPI 扩展。

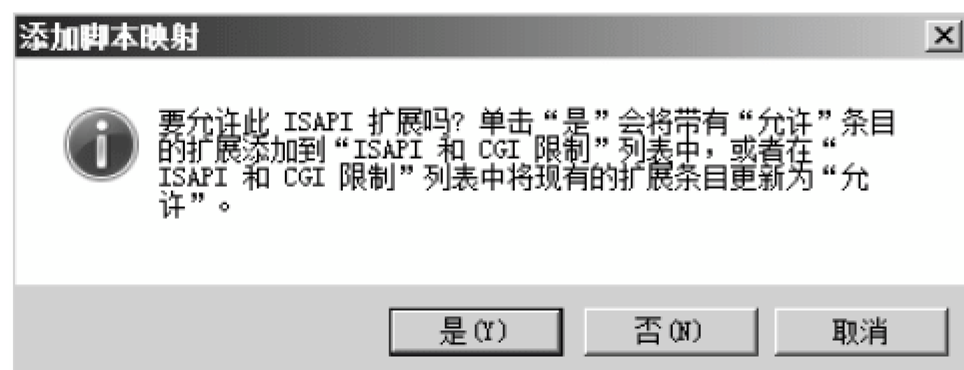
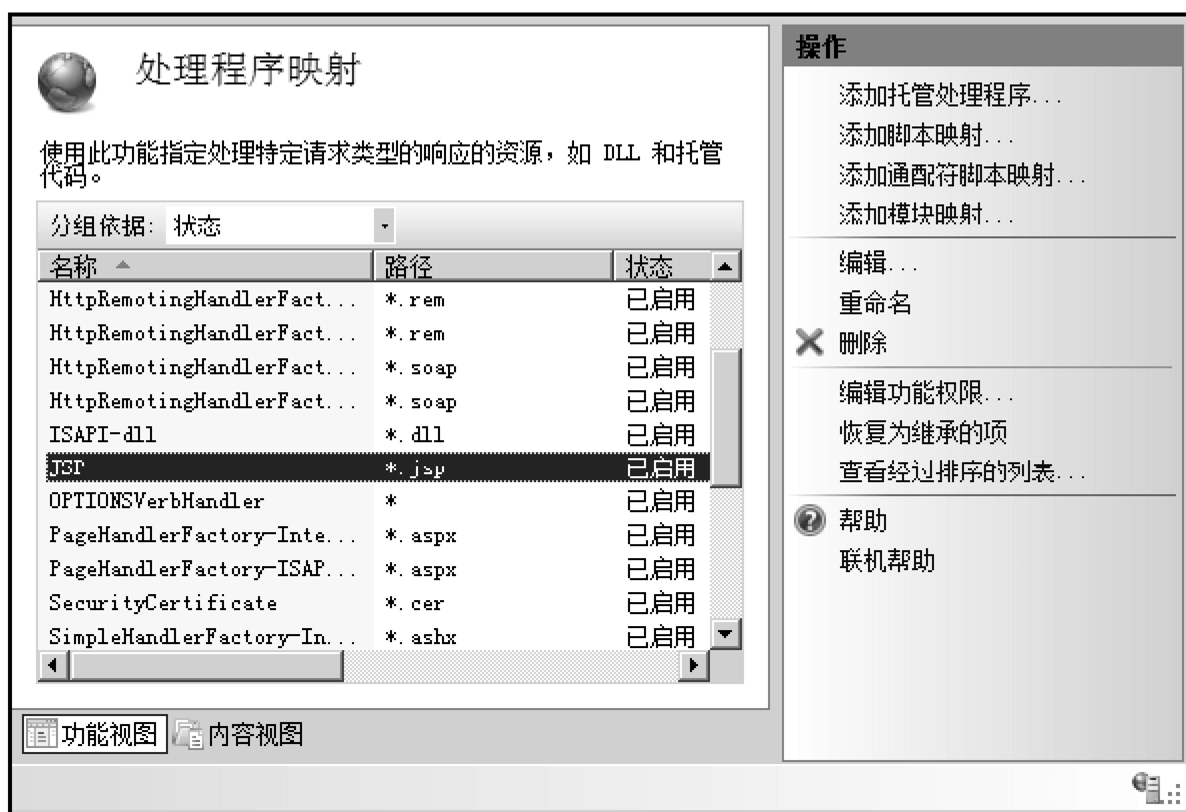


图 10-71 【添加脚本映射】提示框

23 返回至【Internet 信息服务（IIS）管理器】窗口，在【处理程序映射】窗格中选中上文中添加的脚本映射 JSP，选择右侧的【编辑功能权限】选项，如图 10-72 所示。

24 弹出【编辑功能权限】对话框，如图 10-73 所示，选中【读取】、【脚本】和【执行】复选框，单击【确定】按钮。



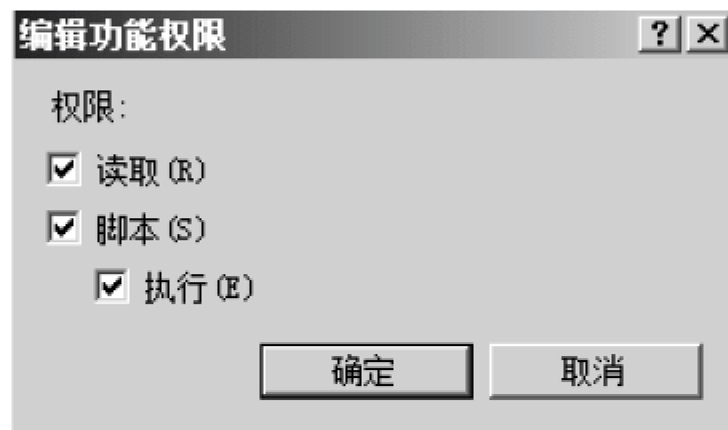


图 10-72 编辑添加的 JSP 脚本映射权限　　图 10-73 【编辑功能权限】对话框

25 返回至【Internet 信息服务（IIS）管理器】窗口，选中左侧【默认站点】选项，双击【默认站点主页】窗格下的【MIME 类型】图标。

26 如图 10-74 所示，选择右侧【添加】选项。



图 10-74　添加 MIME 类型

27 弹出【添加 MIME 类型】对话框，在【文件扩展名】文本框中输入“jsp”，在【MIME 类型】文本框中输入“vapplication/octet-stream”，如图 10-75 所示，单击【确定】按钮。

29 返回至【Internet 信息服务（IIS）管理器】窗口，右击【默认站点】选项，在弹出的快捷菜单中选择【添加虚拟目录】命令。



图 10-75　【添加 MIME 类型】对话框

30 弹出【添加虚拟目录】对话框，在【别名】文本框中输入“jakarta”，在物理路径中输入 JK 文件所在的目录的物理路径，如图 10-76 所示，本实例为“C: \Users\Administrator\Desktop”，单击【确定】按钮。

31 返回至【Internet 信息服务（IIS）管理器】窗口，选中 jakarta 虚拟目录，双击【jakarta 主页】窗格下的【处理程序映射】图标。



图 10-76　【添加虚拟目录】对话框

32 如图 10-77 所示，选择右侧【编辑功能权限】选项。

33 弹出【编辑功能权限】对话框，选中【读取】、【脚本】和【执行】复选框，单击【确定】按钮。

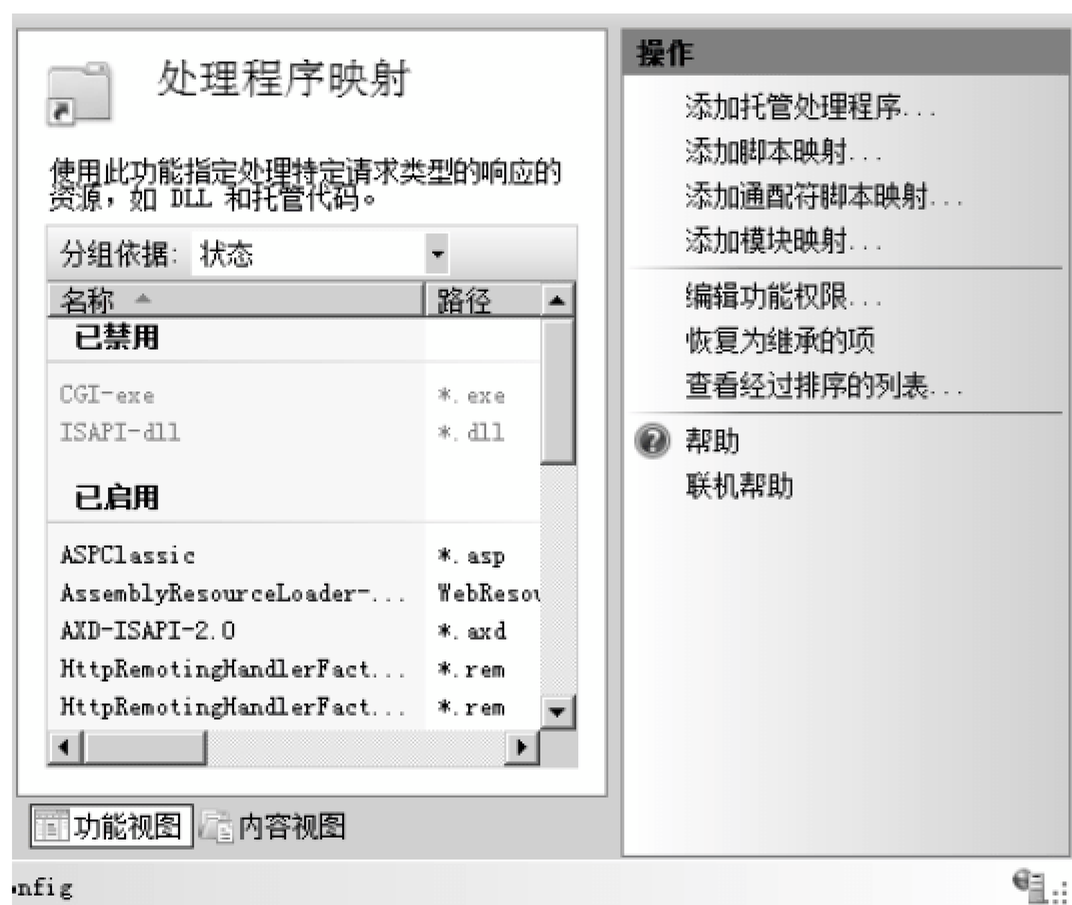


图 10-77 编辑处理程序映射的功能权限

35 返回至【Internet 信息服务（IIS）管理器】窗口，双击左侧【默认站点】选项，双击【默认站点主页】窗格下的【默认文档】图标。

36 如图 10-78 所示，选择右侧【添加】选项。

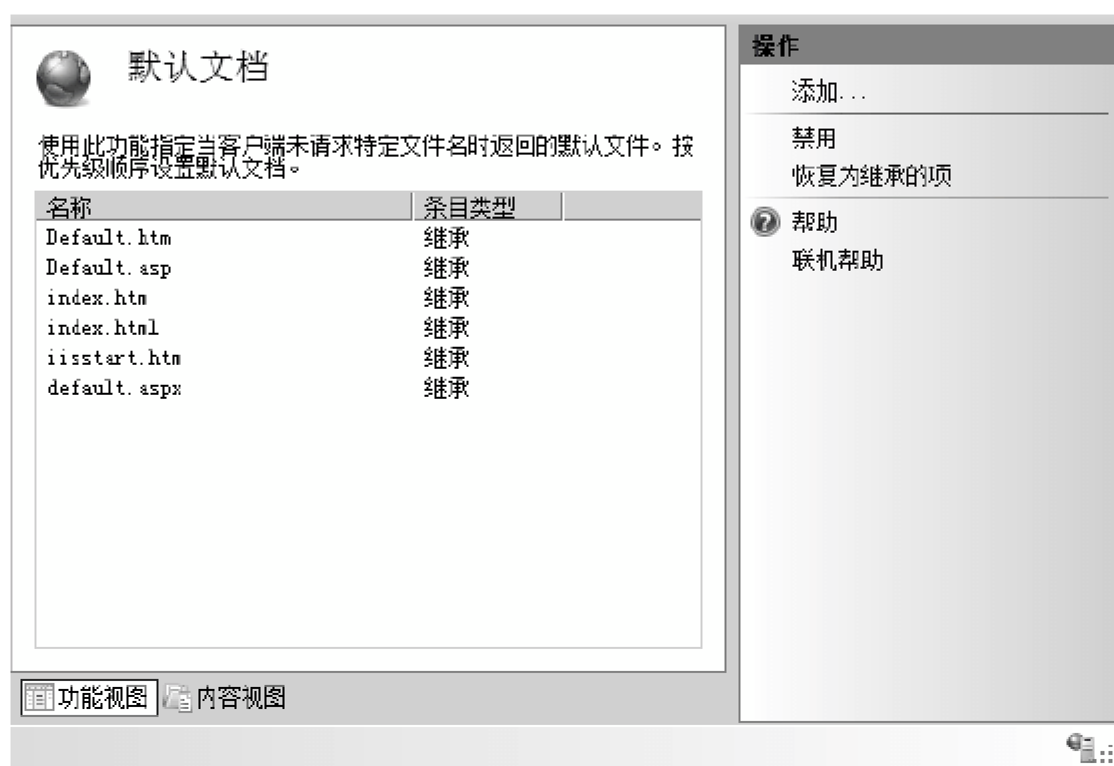


图 10-78 添加新的默认文档

37 弹出【添加默认文档】对话框，在【名称】文本框中输入网站主页的名称，如图 10-79 所示，本实例为“index.jsp”，单击【确定】按钮。

38 用记事本打开 Tomcat 安装路径下的一个文件，该文件的物理路径为“C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf\server.xml”，假如上文新建的目录“myapp”路径是“C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps\myapp”，则在 server.xml 文件的</Host>标签前面加上一行：<Context path="" reloadable="true" docBase="C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps\myapp" workDir="C:\Program Files\Apache Software Foundation\Tomcat 6.0\Web apps\myapp\work" />，本步骤的作用是更改 Tomcat 的默认站

点主目录。

39 重启 Tomcat，右击桌面右下角 Tomcat 图标，在弹出的快捷菜单中选择 Stop service 命令，然后选择 Start service 命令。



图 10-79　【添加默认文档】对话框

40 打开 IE 浏览器，分别在地址栏中输入“http://127.0.0.1”和“http://127.0.0.1:8080”，按 Enter 键，查看结果是否一样，如图 10-80 和图 10-81 所示，如果结果一样则表示发布 JSP 动态网站成功。

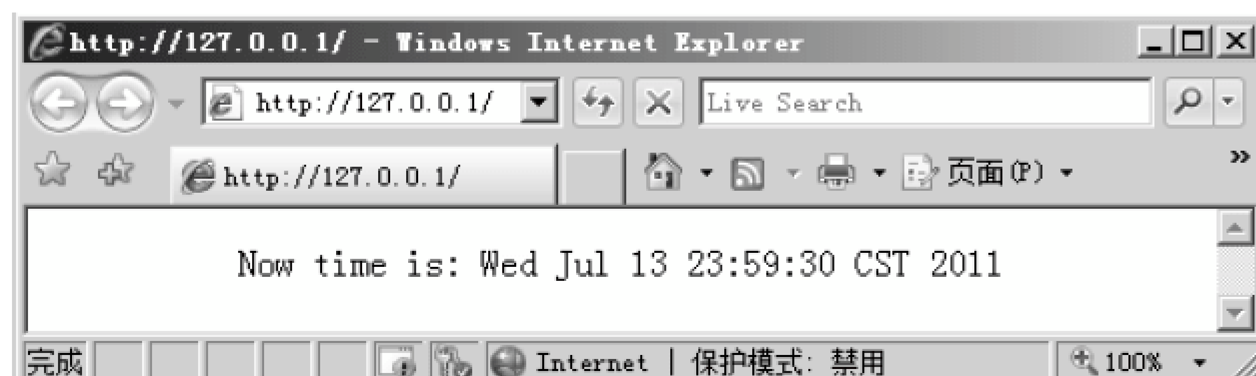


图 10-80　IIS 发布网站

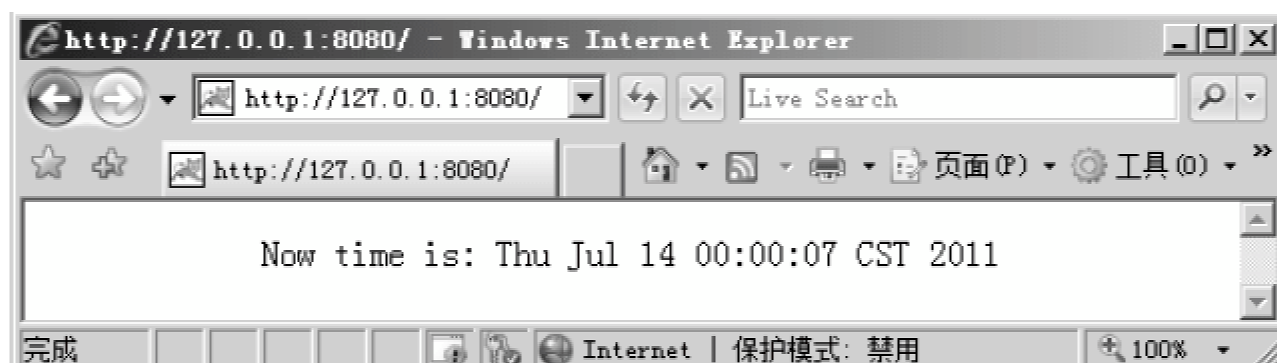


图 10-81　Tomcat 发布网站

10.3　发布 PHP 动态网站

PHP 是最新流行的一款擅长编写网站的脚本语言，目前已成为网页编程语言的主流，使用 IIS 发布 PHP 动态网站的具体操作步骤如下。

10.3.1　安装 MySQL

MySQL 作为开源的数据库软件，和 PHP 结合成为网站开发的黄金搭档，安装 MySQL 的具体操作步骤如下。

01 双击 MySQL 安装文件，如图 10-82 所示，弹出 MySQL 安装向导对话框，单击 Next 按钮。

02 弹出 Setup Type 对话框，如图 10-83 所示，选中 Typical 单选按钮，单击 Next 按钮。



图 10-82　MySQL 安装向导对话框



图 10-83　Setup Type 对话框

03 弹出 Ready to Install the Program 对话框，如图 10-84 所示，单击 Install 按钮。

04 弹出 Installing MySQL Srever 5.0 对话框，如图 10-85 所示，显示 MySQL 安装进度，并显示安装进度条。

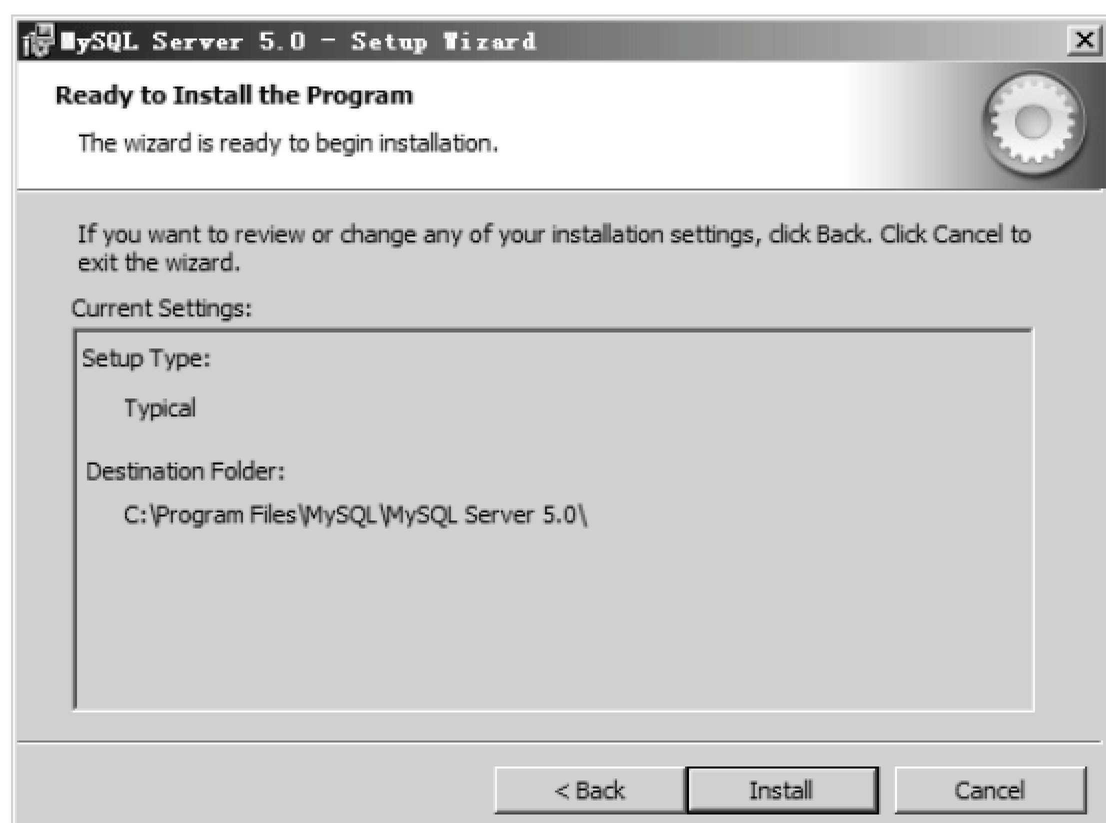


图 10-84　Ready to Install the Program 对话框



图 10-85　Installing MySQL Srever5.0 对话框

05 弹出 MySQL Enterprise 对话框，如图 10-86 所示，单击 Next 按钮。

06 弹出 MySQL Monitoring 对话框，如图 10-87 所示，单击 Next 按钮。

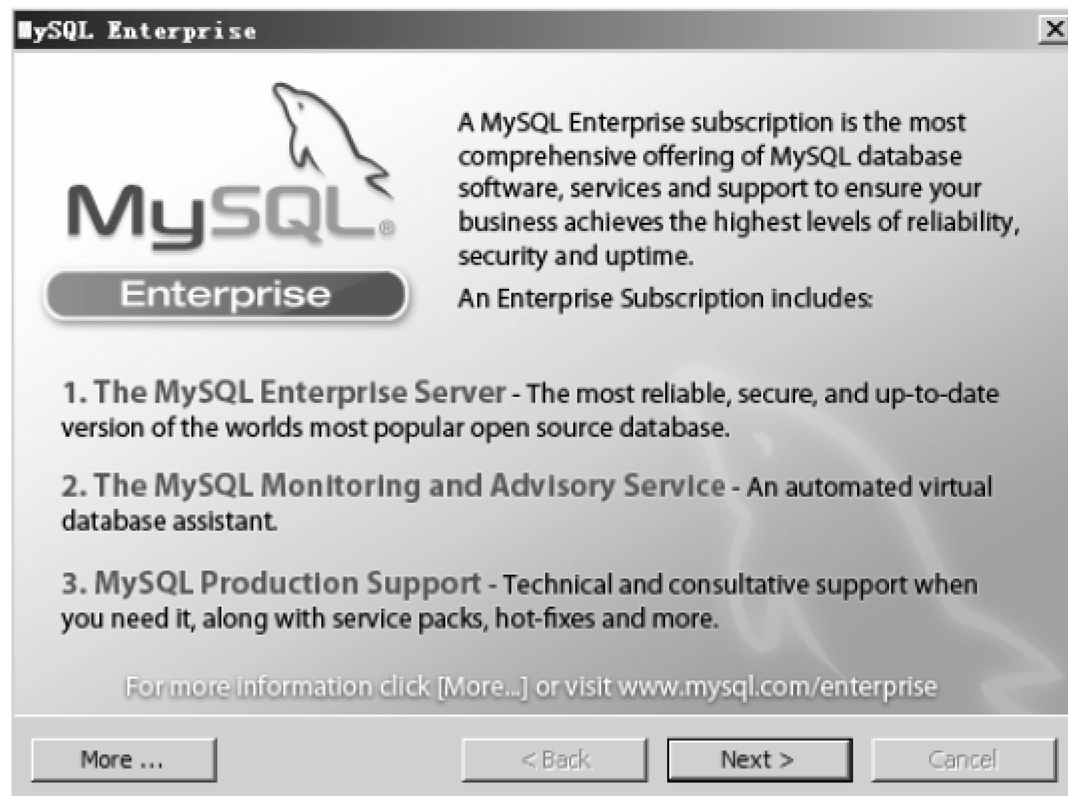


图 10-86　MySQL Enterprise 对话框



图 10-87　MySQL 监控服务对话框

07 弹出 Wizard Completed 对话框，如图 10-88 所示，选中 Configure the MySQL Server now 复选框，单击 Finish 按钮。

08 弹出 MySQL Server Instance Configuration Wizard 对话框，如图 10-89 所示，单击 Next 按钮。

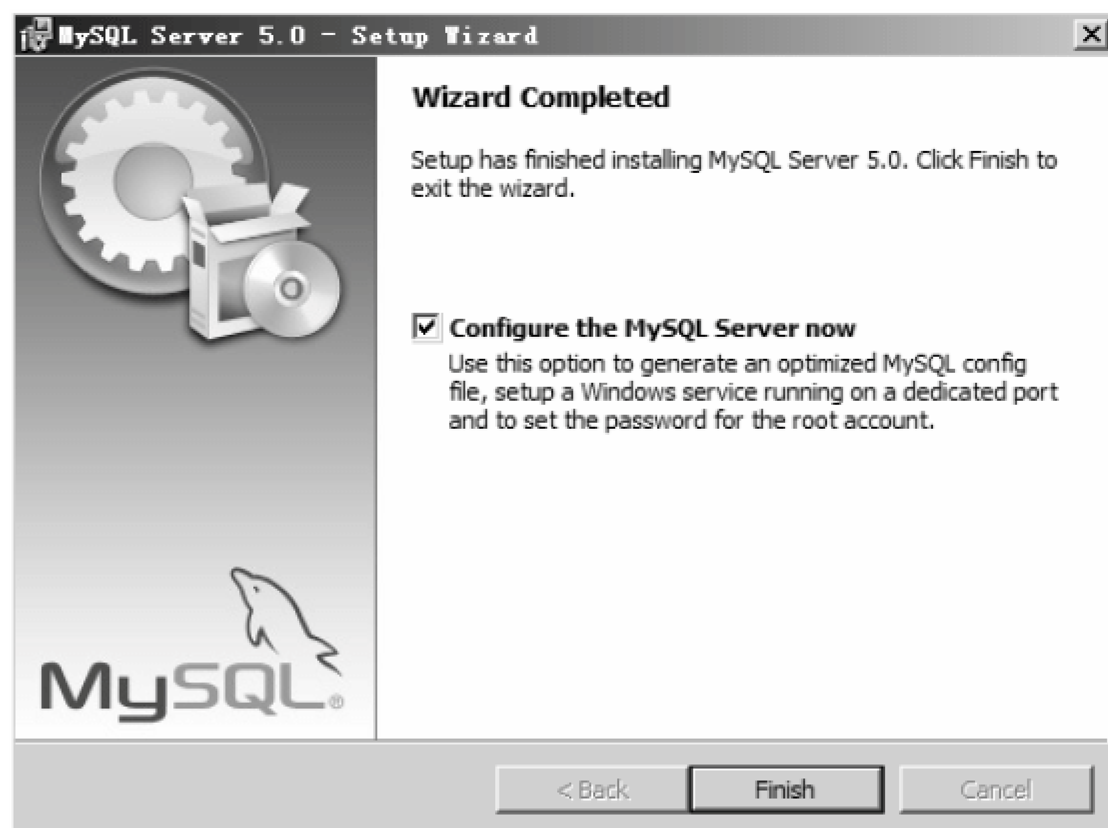


图 10-88 Wizard Completed 对话框



图 10-89 MySQL 服务器配置向导对话框

09 弹出 MySQL Server Instance Configuration 对话框，如图 10-90 所示，选中 Detailed Configuration 复选框，单击 Next 按钮。

10 弹出服务类型对话框，如图 10-91 所示，选择 MySQL 的运行模式，选中 Server Machine 单选按钮，单击 Next 按钮。

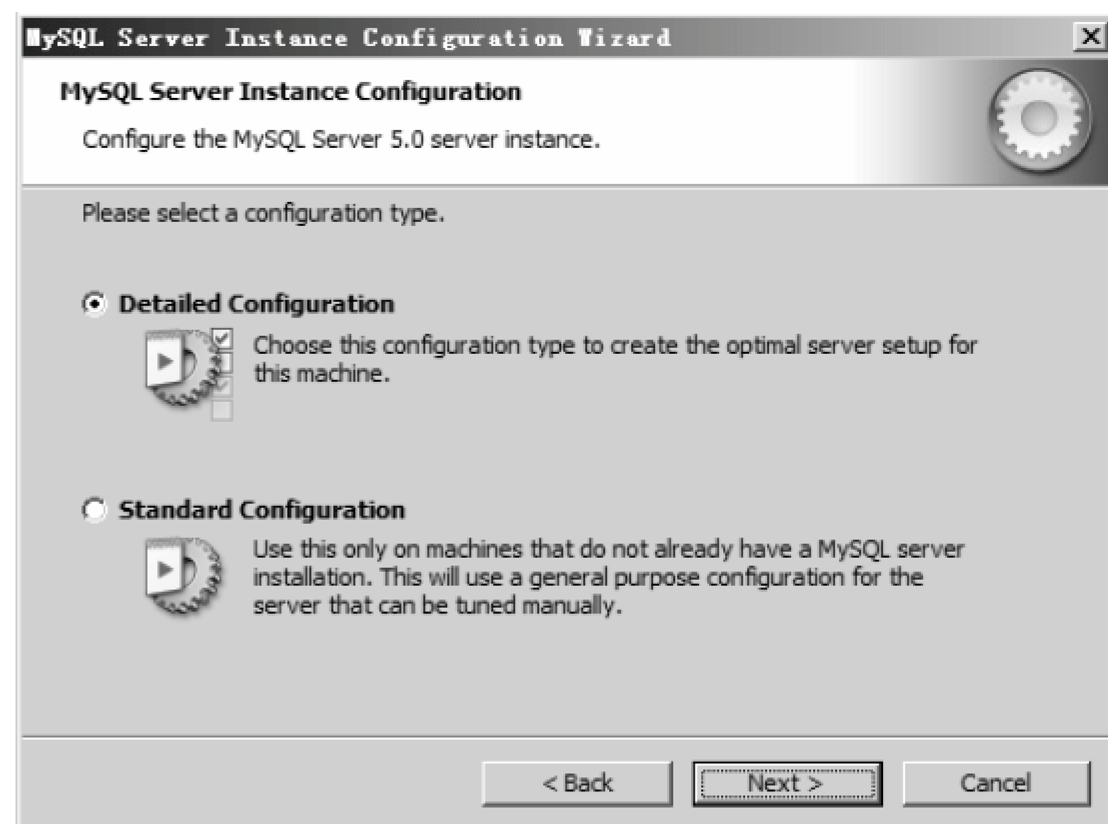


图 10-90 MySQL Server Instance Configuration 对话框



图 10-91 选择 MySQL 的运行模式

11 弹出数据存储方式对话框，如图 10-92 所示，选中 Non-Transactional Database Only 单选按钮，单击 Next 按钮。

12 弹出服务器连接数对话框，如图 10-93 所示，选中 Manual Setting 单选按钮，在 Concurrent connections 文本框中输入“150”，表示默认情况下同时允许 150 个用户连接 MySQL 服务器。

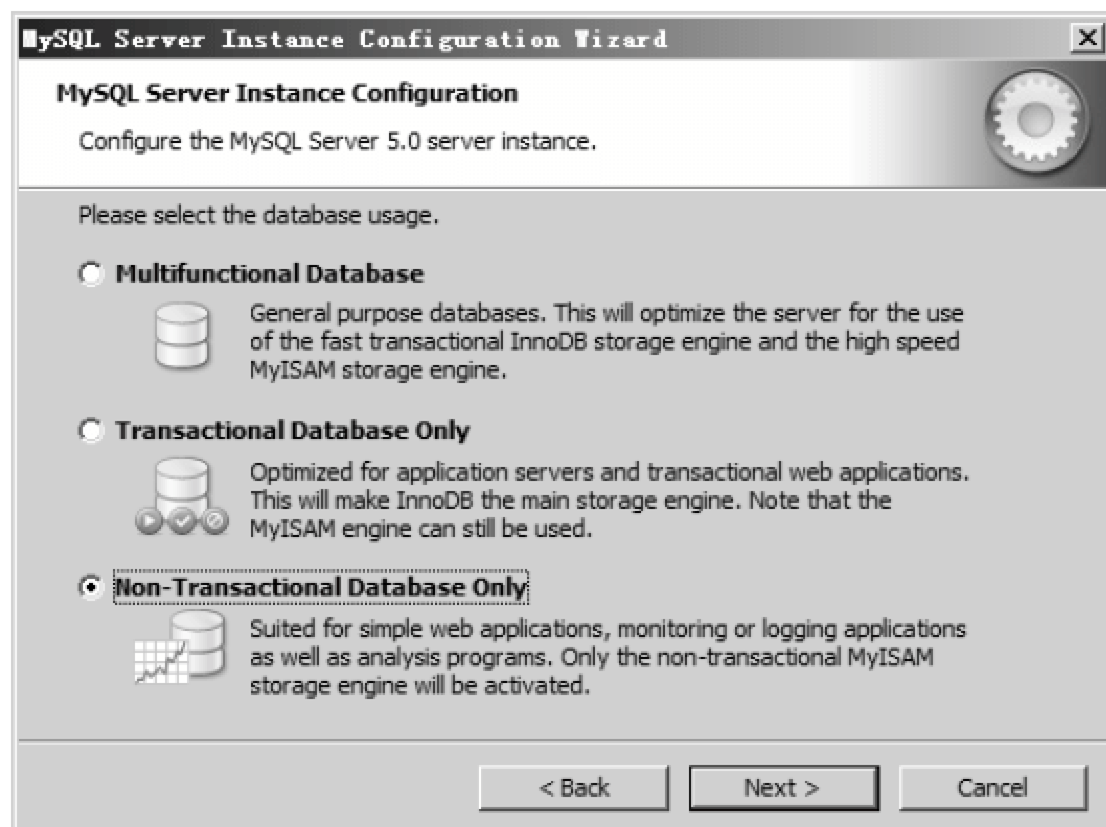


图 10-92　选择数据存储方式

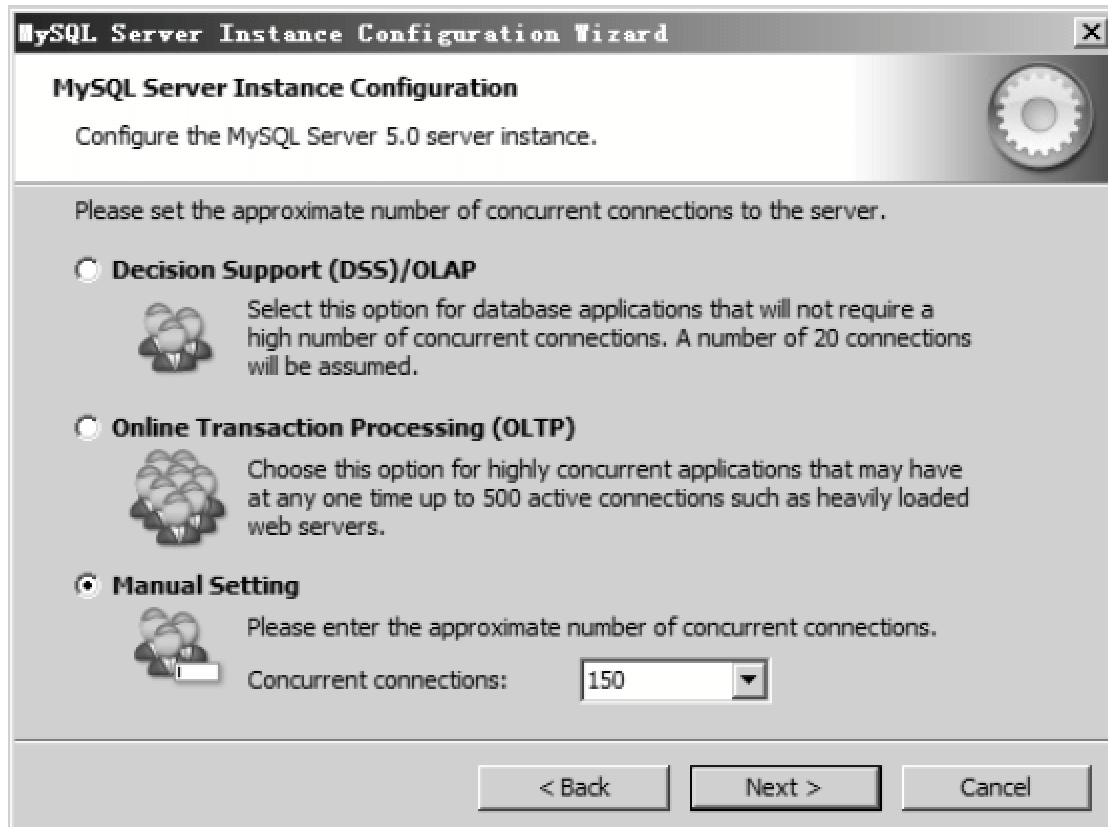


图 10-93　设置服务器连接数

13 弹出网络选项对话框，如图 10-94 所示，选中 Enable TCP/IP Networking 复选框，单击 Next 按钮。

14 弹出字符设置对话框，如图 10-95 所示，选中 Manual Selected Default Character Set /Collation 单选按钮，在 Character Set 下拉列表框中选择 gbk，单击 Next 按钮。

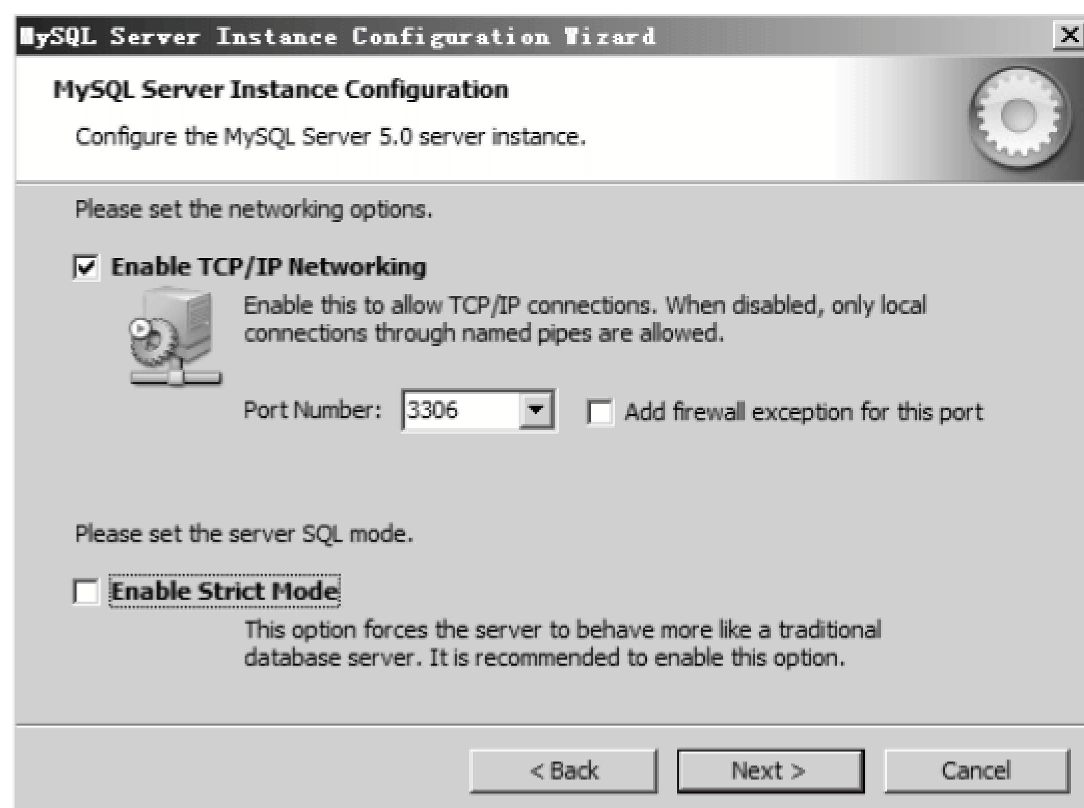


图 10-94　选择网络模式

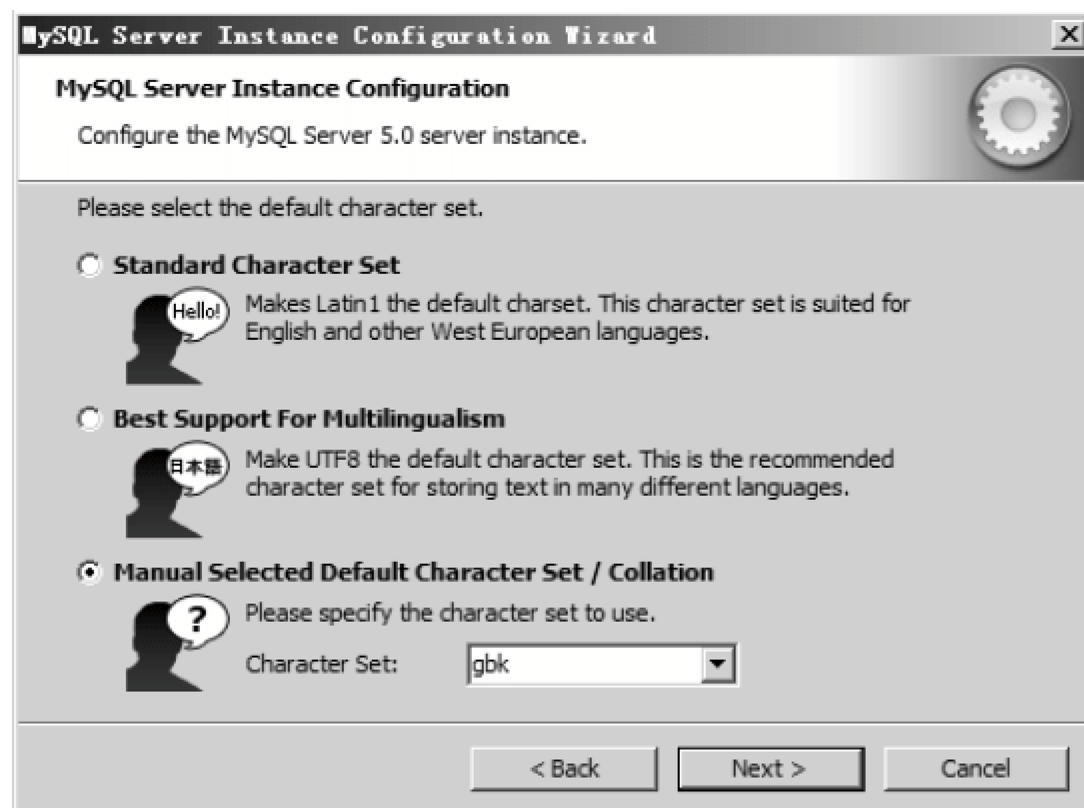


图 10-95　字符设置

15 弹出 Windows 选项对话框，如图 10-96 所示，选中 Install As Windows Service 复选框，单击 Next 按钮。

16 弹出安全选项对话框，如图 10-97 所示，选中 Modify Security Settings 复选框，在 New root password 和 confirm 文本框中输入管理员 root 的密码，单击 Next 按钮。

17 弹出准备执行对话框，如图 10-98 所示，单击 Execute 按钮。

18 弹出进程配置对话框，如图 10-99 所示，显示配置进度。



图 10-96　Windows 选项对话框



图 10-97　安全选项对话框

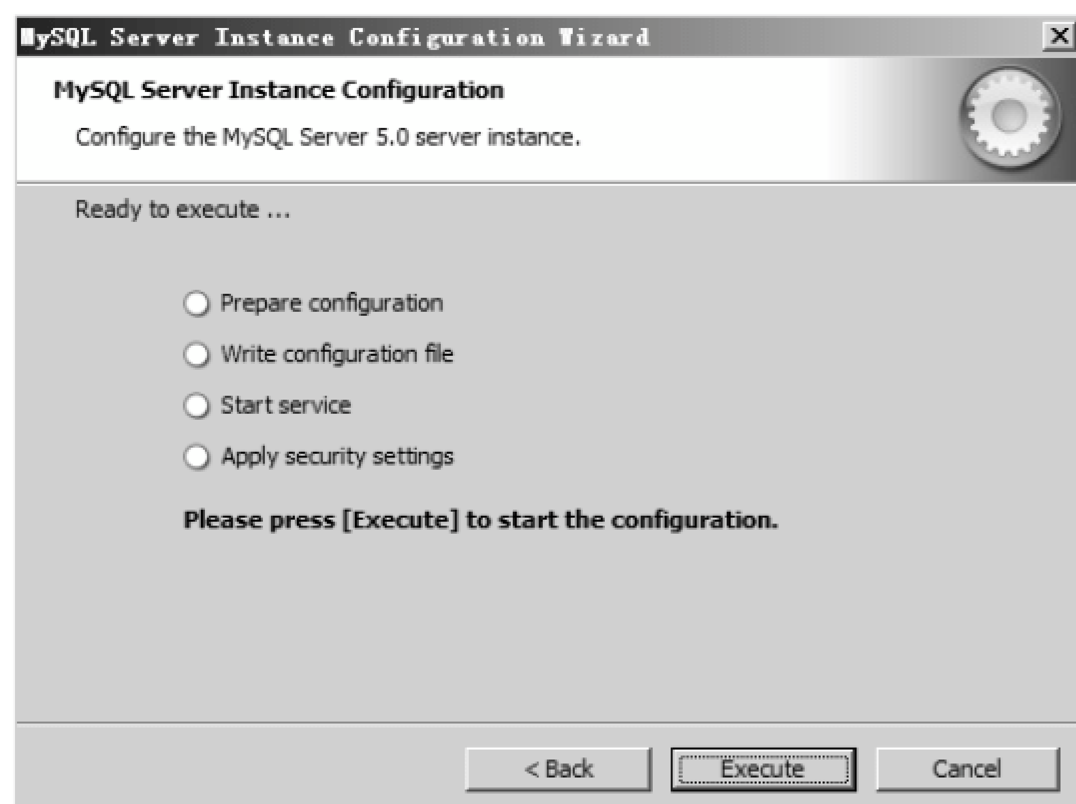


图 10-98　准备执行对话框

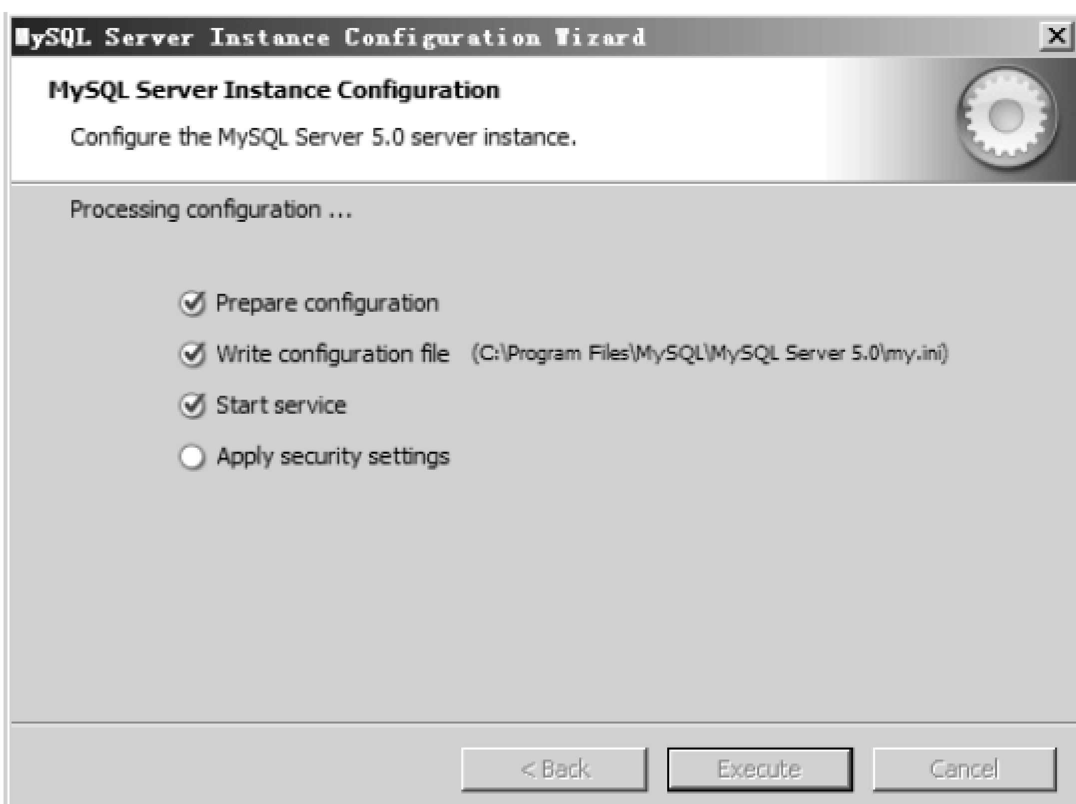


图 10-99　进程配置对话框

19 弹出完成对话框，如图 10-100 所示，单击 Finish 按钮。

20 测试 MySQL 是否正常工作，选择【开始】➢【运行】命令，弹出【运行】对话框，在【打开】文本框中输入命令 cmd，单击【确定】按钮。

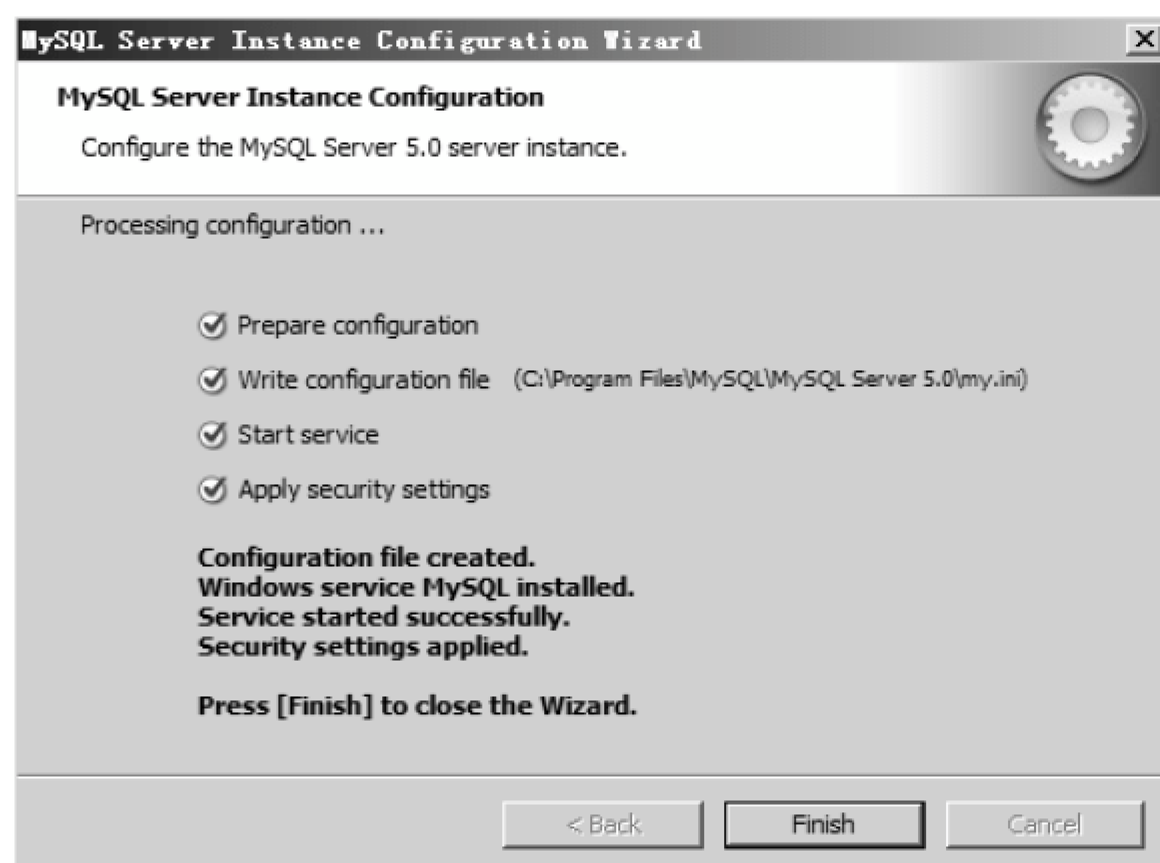


图 10-100　完成对话框

21 弹出 cmd 窗口，如图 10-101 所示，在光标处输入命令“mysql –u root -p”，按 Enter 键。

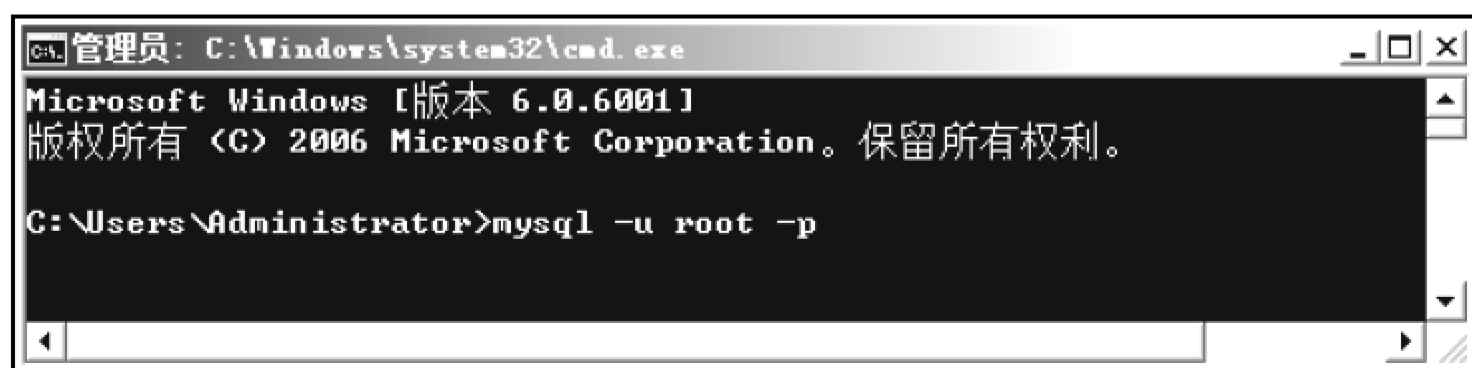


图 10-101 cmd 窗口

22 在 Enter password 后面输入用户“root”的密码，本实例中密码为“sushi@163.com”，按 Enter 键。

23 如图 10-102 所示，进入 MySQL 配置模式，表示 MySQL 正常工作，输入命令“net stop mysql”，按 Enter 键，停止 MySQL 工作。



图 10-102 MySQL 配置模式

24 更改 MySQL 的数据库存储位置。打开 MySQL 的配置文件，MySQL 配置文件的物理路径为“C:\Program Files\MySQL\MySQL Server 5.0\my.ini”，如图 10-103 所示，将该配置文件中的“datadir = " C:\Program Files\MySQL\MySQL Server 5.0\data"”修改为“datadir = "C:\Database\"”，然后进行保存。

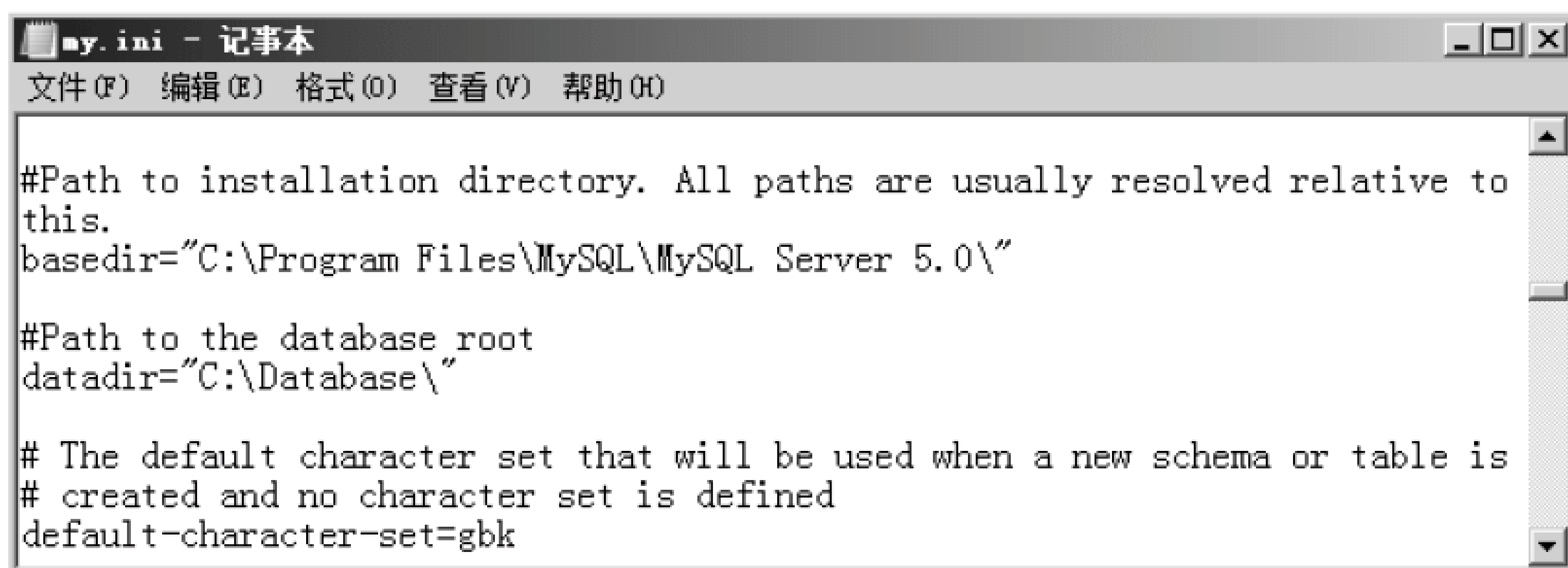


图 10-103 更改数据库存储位置

25 保存数据库文件，将“C:\Program Files\MySQL\MySQL Server 5.0\data” 文件夹复制到“C:\”中并重命名为“C:\Database”。

26 准备 LibMySQL 动态链接库，将“C:\Program Files\MySQL\MySQL Server 5.0\bin\libMySQL.dll ”文件复制到 “C:\Windows\System32” 。

27 重新测试 MySQL 是否正常运行。选择【开始】➢【运行】命令，弹出【运行】对话框，在【打开】文本框中输入命令“cmd”，单击【确定】按钮。

28 弹出 cmd 窗口，在光标处输入命令“mysql –u root -p”，按 Enter 键。

29 在 Enter password 后面输入用户“root”的密码 sushi@163.com，按 Enter 键。

30 如图 10-104 所示，进入 MySQL 配置模式，表示 MySQL 正常工作，输入命令“net start mysql”，按 Enter 键，启动 MySQL，表示 MySQL 正常工作。



图 10-104　MySQL 配置模式

10.3.2　安装 PHP

在 Windows 系统上配置 PHP 语言的具体操作步骤如下。

01 双击 PHP 压缩文件，如图 10-105 所示，单击【提取所有文件】按钮。

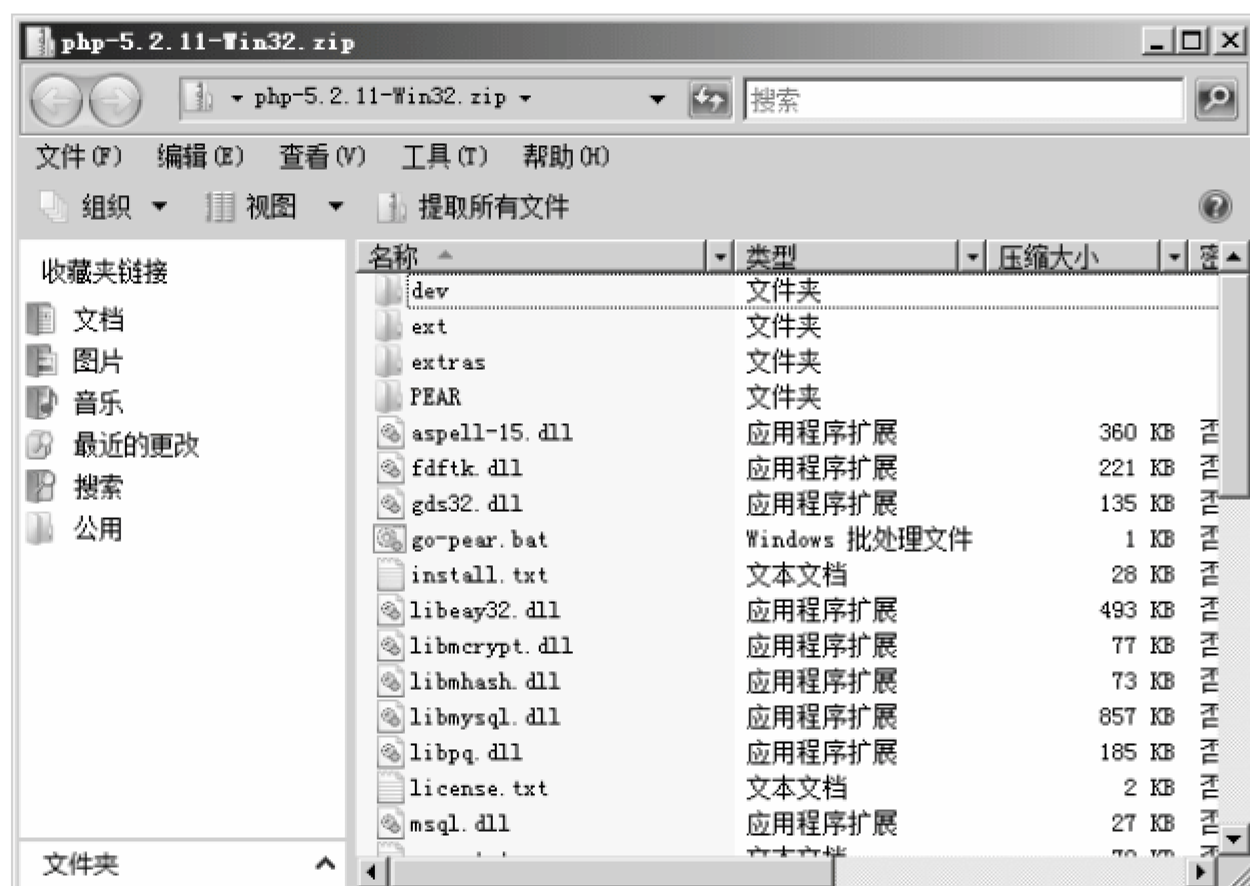


图 10-105　PHP 压缩文件

02 弹出【提取压缩（Zipped）文件夹】对话框，如图 10-106 所示，单击【浏览】按钮。

03 弹出【选择一个目标】对话框，浏览找到 PHP 的安装路径，本实例根据需要选择的 PHP 的安装路径为“C:\Program Files\php”，如果 php 目录不存在，需要事先建立，如图 10-107 所示，单击【确定】按钮。



图 10-106 【提取压缩（Zipped）文件夹】对话框

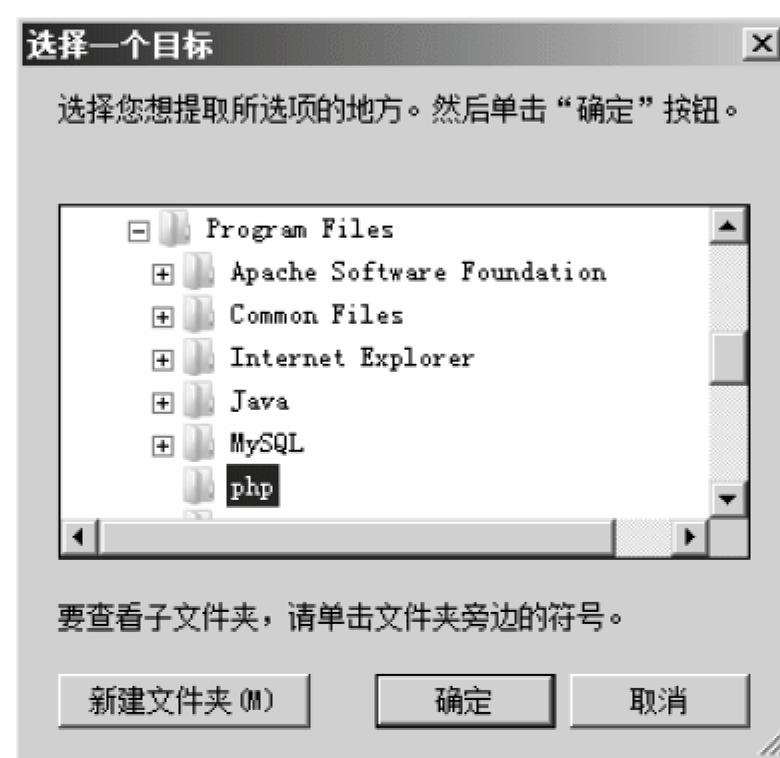


图 10-107 【选择一个目标】对话框

04 返回至【提取压缩（Zipped）文件夹】对话框，单击【确定】按钮。

05 弹出【正在复制】提示框，显示 PHP 提取进度，并显示提取进度条。

06 将 PHP 安装目录中的“php.ini-dist”文件重命名为“php.ini”，PHP 安装目录的物理路径为“C:\Program Files\php”。

07 打开 PHP 配置文件，PHP 配置文件物理路径为“C:\Program Files\php\php,ini”，将 PHP 配置文件中“extension_dir = "./" ”修改为 extension_dir = "C:\Program Files\php\ext"，将“disable_functions =”修改为“disable_functions=phpinfo,passthru,exec,system,chroot,scandir,chgrp,chown,shell_exec,proc_open,proc_get_status,ini_alter,ini_restore,dl,pfsockopen,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server”，在“Windows Extensions”下方的动态模块配置中，需要打开以下模块支持（去掉模块配置每行前面的“;”号即可）:

```
extension=php_mbstring.dll
extension=php_gd2.dll
extension=php_mysql.dll
```

08 保存上一步骤修改过的 PHP 配置文件后，然后将 PHP 配置文件“php.ini”复制至“C:\Windows”目录中。

10.3.3 IIS 与 PHP 的整合配置——发布 PHP 动态网站

当 Web 服务器上的 PHP 和 MySQL 安装配置完成后，将 IIS 和 PHP 整合在一起，进行 PHP 动态网站的发布，使用 IIS 发布 PHP 动态网站的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【Internet 信息服务（IIS）管理器】选项，弹出【Internet 信息服务（IIS）管理器】窗口，双击 WIN-013D26R8BJX，右击【网站】选项，在弹出的快捷菜单中选择【添加网站】命令。

02 弹出【添加网站】对话框，在【网站名称】文本框中输入网站名称为“php”，如图 10-108 所示，单击【物理路径】文本框后面的...按钮。

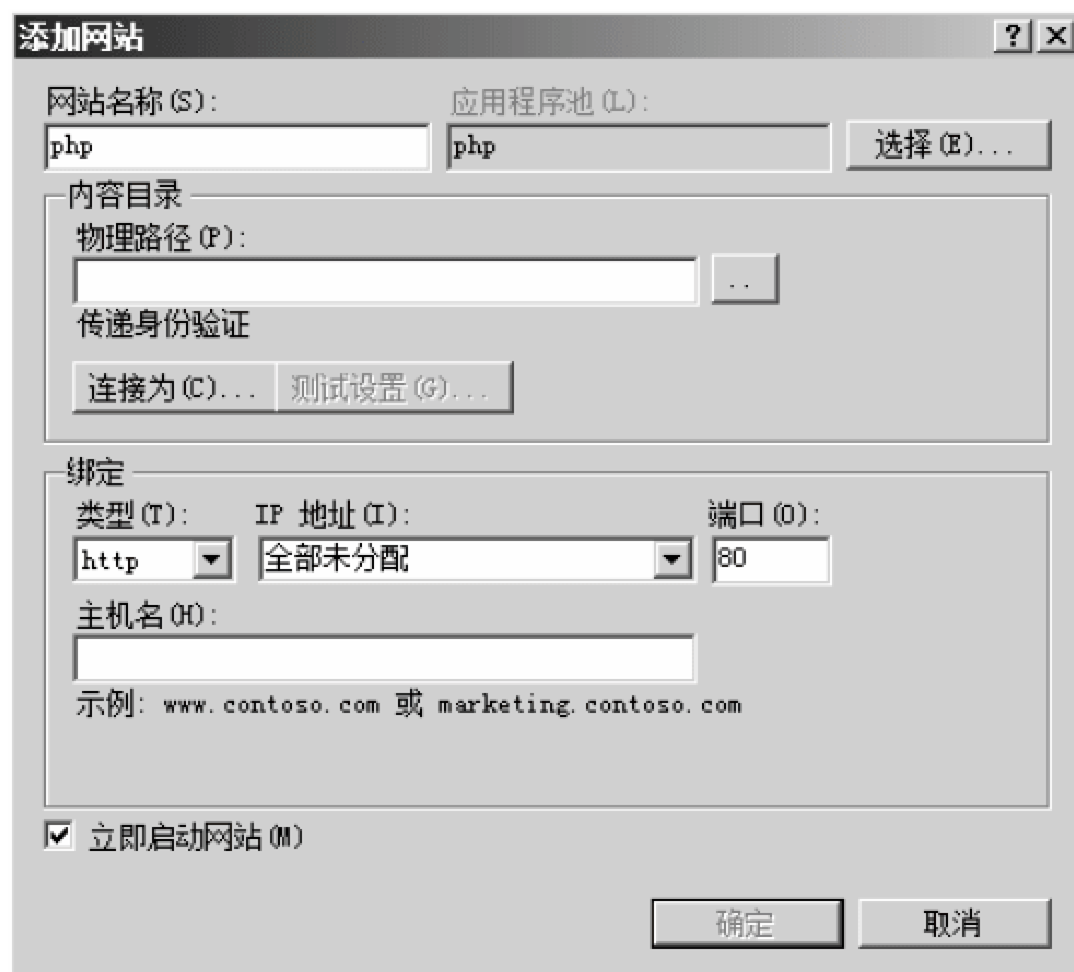


图 10-108　【添加网站】对话框

03 弹出【浏览文件夹】对话框，浏览选择 PHP 网站所在的目录，如图 10-109 所示，本实例为 PHP 网站的主目录物理路径为 “C:\php” ，单击【确定】按钮。

04 返回至【添加网站】对话框，选中【立即启用网站】复选框，注意这里 PHP 网站使用 80 端口，应该将其他使用 80 端口的网站删除掉，单击【确定】按钮。

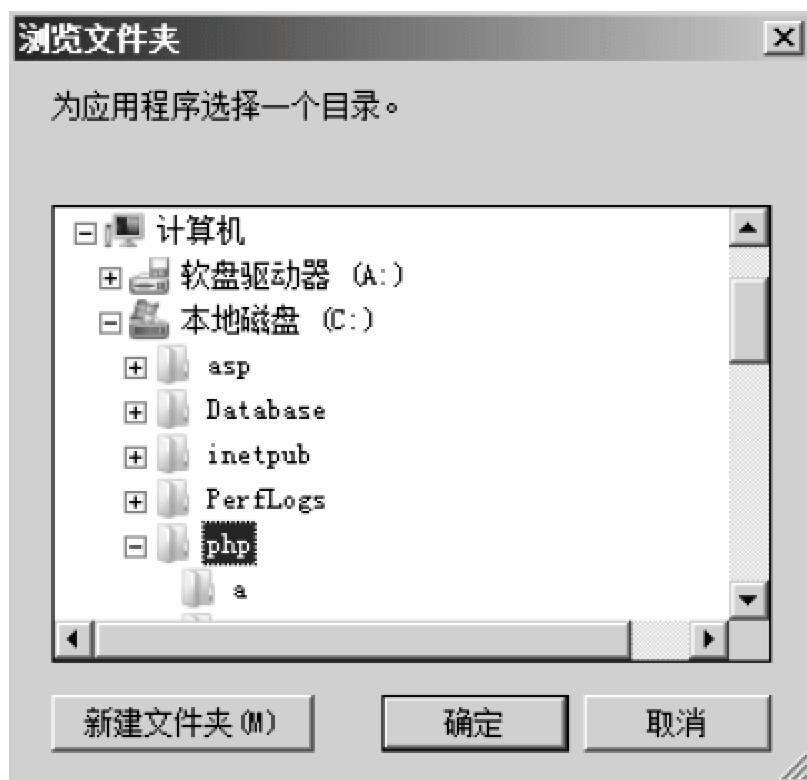


图 10-109　【浏览文件夹】对话框

05 返回至【Internet 信息服务（IIS）管理器】窗口，双击左侧 WIN-013D26R8BJX 选项，再双击【ISAPI 和 CGI 限制】图标。

06 弹出【ISAPI 和 CGI 限制】窗格，选择右侧【添加】选项。

07 弹出【添加 ISAPI 或 CGI 限制】对话框，单击【ISAPI 或 CGI 路径】文本框后面的 .. 按钮。

08 弹出【打开】对话框，浏览找到本地的 PHP 连接文件，PHP 连接文件在 PHP 的安装目录中，本实例中 PHP 连接文件的物理路径为 “C:\Program Files\php\php5isapi.dll” ，单击【打开】按钮。

09 返回至【添加 ISAPI 或 CGI 限制】对话框，在【描述】文本框中输入 “PHP 连接 IIS” ，选中【允许执行扩展路径】复选框，单击【确定】按钮。

10 返回至【Internet 信息服务（IIS）管理器】窗口，选择【网站】➢【php】选项，双击【php

主页】窗格中的【ISAPI 筛选器】图标。

11 打开【ISAPI 筛选器】窗格，如图 10-110 所示，选择右侧【添加】选项。

12 弹出【添加 ISAPI】筛选器，在【筛选器名称】文本框中输入 “jakarta” ，在【可执行文件】文本框中输入 PHP 连接文件 “php5isapi.dll” 的物理绝对路径，如图 10-111 所示，本实例为 “C:\Program Files\php\php5isapi.dll” ,单击【确定】按钮。

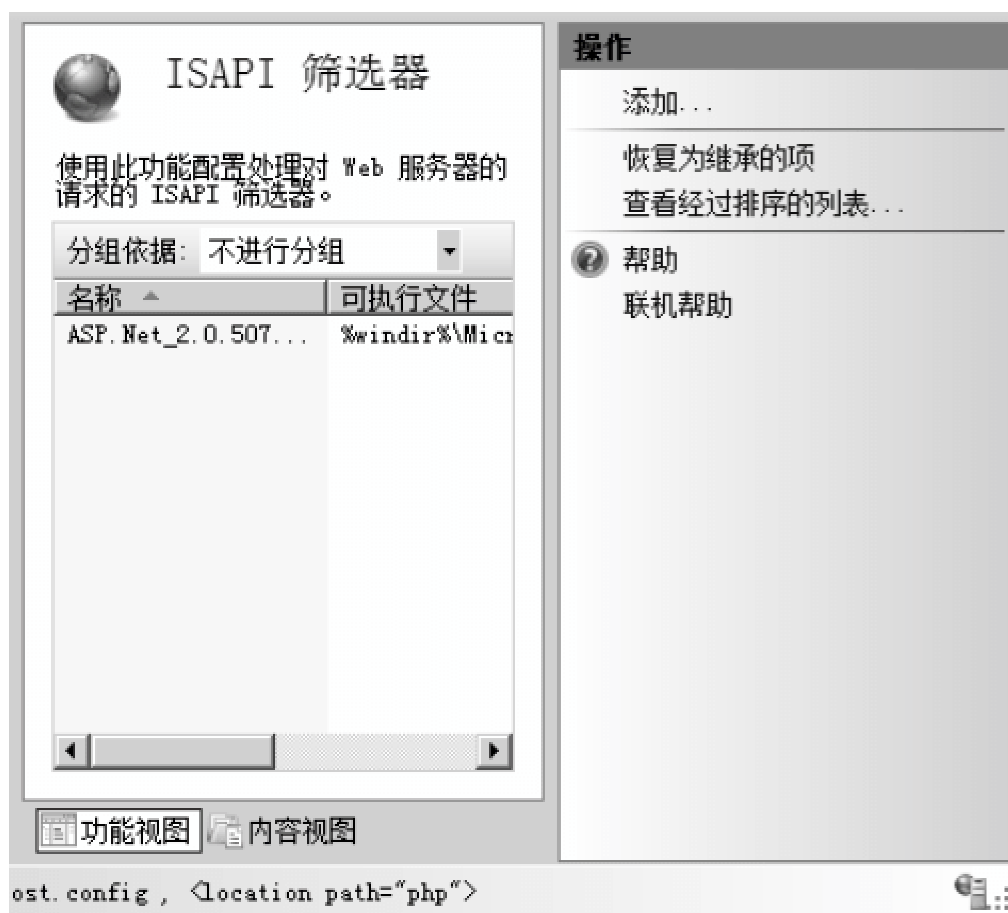


图 10-110 【ISAPI 筛选器】窗格

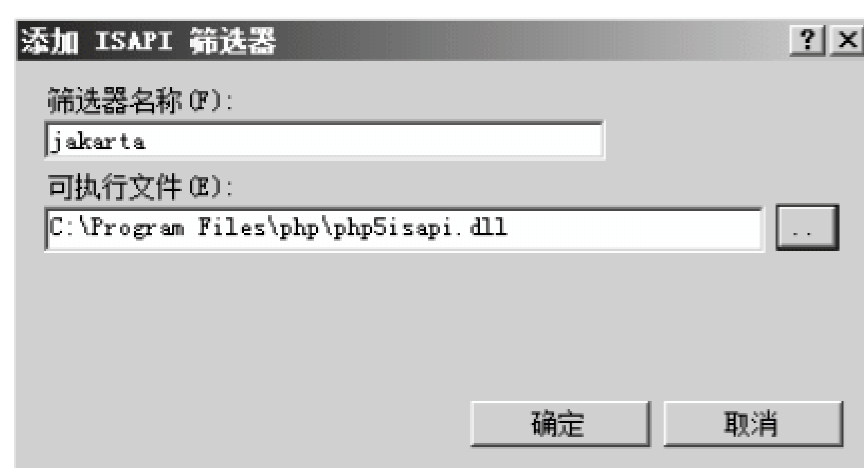


图 10-111 【添加 ISAPI 筛选器】对话框

13 返回至【Internet 信息服务（IIS）管理器】窗口，双击 php 选项，然后单击【php 主页】窗格下的【处理程序映射】图标。

14 在【php 主页】窗格右侧选择【添加脚本映射】选项。

15 弹出【添加脚本映射】对话框，在【请求路径】文本框中输入 “*.php” ，单击【可执行文件】文本框后面的 .. 按钮。

16 弹出【打开】对话框，浏览找到 PHP 连接文件，本实例 JK 文件物理路径为 “C: \Program Files\php\php5isapi.dll” ，单击【打开】按钮。

17 返回至【添加脚本映射】对话框，该对话框的主要功能是使得 IIS 可以自动识别 php 类型文件，如图 10-112 所示，在【名称】文本框中输入 “PHP” ，单击【确定】按钮。

18 弹出【添加脚本映射】提示框，单击【是】按钮，表示同意添加此 ISAPI 扩展。

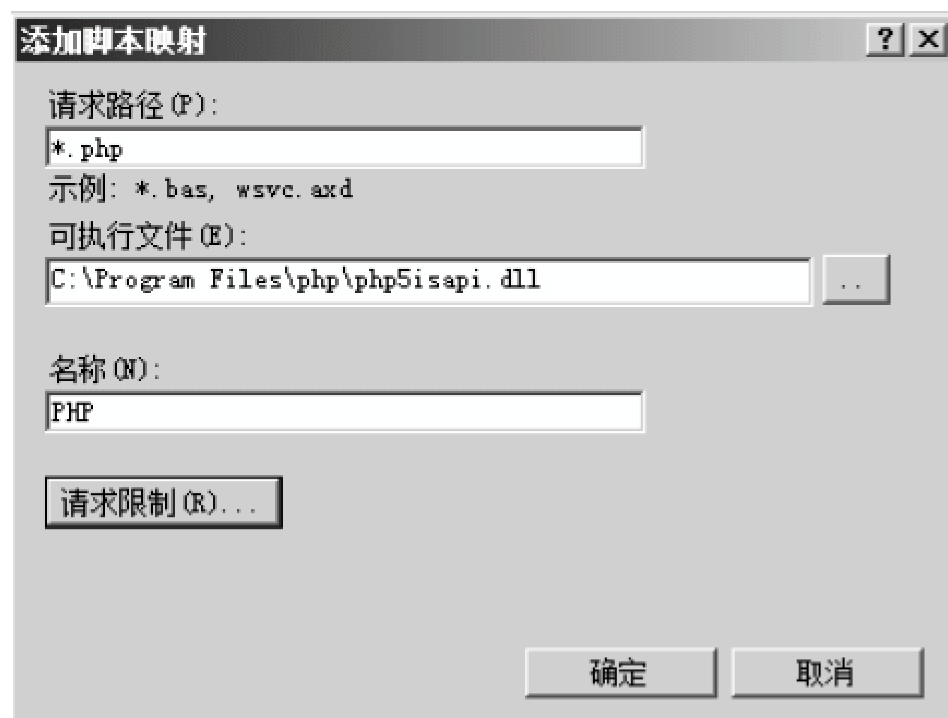


图 10-112 【添加脚本映射】提示框

19 返回至【Internet 信息服务（IIS）管理器】窗口，如图 10-113 所示，选中上文中添加的脚本映射【PHP】，单击右侧的【编辑功能权限】选项。

20 弹出【编辑功能权限】对话框，选中【读取】、【脚本】和【执行】复选框，单击【确定】按钮。



图 10-113　配置新加 PHP 脚步映射的功能权限

21 返回至【Internet 信息服务（IIS）管理器】窗口，双击选中左侧 php 选项，双击 php 窗格下的【MIME 类型】图标，

22 在【MIME 类型】窗格右侧选择【添加】选项。

23 弹出【添加 MIME 类型】对话框，在【文件扩展名】文本框中输入“.php”，在【MIME 类型】文本框中输入“vapplication/octet-stream”，如图 10-114 所示，单击【确定】按钮。

24 返回至【Internet 信息服务（IIS）管理器】窗口，双击左侧 php 选项，如图 10-115 所示，在右侧选择【添加】选项。



图 10-114　【添加 MIME 类型】对话框



图 10-115　添加默认文档

25 弹出【添加默认文档】对话框，在【名称】文本框中输入 PHP 网站的主页名称，如图 10-116

所示，本实例 PHP 网站主页名称为“index.php”，单击【确定】按钮。

26 返回至【Internet 信息服务（IIS）管理器】窗口，右击 php 选项，在弹出的快捷菜单中选择【管理网站】➢【浏览】命令。



图 10-116 【添加默认文档】对话框

27 如图 10-117 所示，打开 PHP 网站成功，表示 PHP 动态网站发布成功。



图 10-117 PHP 动态网站

10.4 专家答疑

（1）发布企业级动态网站需要配置较为复杂的环境变量，有没有更为简便的方法？

答：默认情况下浏览器只能识别静态网页，如果要想识别更为高级的动态语言，必须安装该语言的运行平台并配置环境变量。目前在网络中有发布动态网站的一键安装包，但是这种软件包只能在实验的环境下使用，因为一键安装包的设置和访问流量承载能力都不能满足实际需求，如果使用一键安装包发布动态网站，会给后期的网站维护带来不便。

（2）一台企业服务器是否可以同时发布多种类型的动态网站？

答：各种动态网站技术之间是没有冲突的，一台服务器完全可以配置多种动态网站发布服务。这对于个人企业的网站服务器用处不是很大，因为一个企业一般只有一套网站需要发布，但是对于 IDC 托管机构来说，他们的服务器整体配置很高，为了充分利用资源，同时实现多种类型的动态网站服务是很正常的。

第 11 章　企业服务器的对外发布与管理

配置好的企业 Web 服务器，或者 E-Mail 服务器并不能被互联网用户使用，需要获得公共认可的域名，同时还要将配置好的服务器放置在可被互联网访问到的位置。本章将详细讲解做好的服务器如何在互联网中发布。

11.1　域名注册

域名由国际域名分发机构统计管理，由于使用 IP 地址记录互联网中的各种服务器对人来说太难记忆，所以就产生了域名，域名可以看做是为互联网中各个服务器的 IP 地址取的一个方便记忆的别名，如“baidu.com”。

常见的企业对外发布服务器有 Web 服务器和 E-Mail 服务器，这两个服务器在互联网中被用户访问时都需要使用域名识别其身份和位置，所以对外发布服务器时首先要为其注册域名。本节将详细讲解域名的选择、注册及管理等内容。

11.1.1　域名的选择

选择域名是一项非常重要的工作，好的域名可能会为网站带来更多的访问量，为企业带来更多的利益。

选择域名需要按照以下步骤完成。

第一步：结合自身企业的需求特征拟定几个域名，这些域名要遵循简单、好记、好录入和意义明确的原则。

第二步：去域名注册网站（如万网）查询该域名是否被人注册，被人注册过的域名是不可以使用的。

第三步：如果域名没有被注册，可以通过百度或者 Google 等搜索引擎搜索该域名，查看一下是否有该域名的使用记录，如果有表示该域名曾经被使用过，曾经被使用过的域名被称做老域名，如果认为这个域名还不错的话就可以直接注册了。

好域名非常重要，如果一直拿不定主意的话，可以多分析一下百度、新浪等热门网站的域名。

11.1.2　项目实战 1：注册域名

可以注册域名的网站很多，本实例选择使用万网注册域名，具体操作步骤如下。

01 打开 IE 浏览器，在地址栏中输入“www.net.cn”，打开万网的官方网站，右侧有域名查询模块，如图 11-1 所示。



图 11-1　万网官方主页面

02 打开【域名注册】页面，左侧选项列表中可以选择多项目域名服务内容，下面模块可以进行域名的查询，如图 11-2 所示。



图 11-2　【域名注册】页面

03 在域名查询模块中有三个选项，分别是【中英文域名查询】、【多个域名后缀】和【单个域名后缀】选项，本实例使用【多个域名后缀】，在文本框中输入需要查询的域名，在下侧选择要查询的后缀，然后单击【查询】按钮，如图 11-3 所示。

04 显示域名查询结果，包括域名、注册状态、价格等信息，选择需要购买的域名，单击【所

选域名加入购物车】按钮，如图 11-4 所示。



图 11-3　域名查询模块



图 11-4　域名查询结果

05 打开购物车页面，显示了选购的域名，本实例选购了域名“yinhangit.com”，在【请选择域名所有者类型】选项中有两项，根据申请者身份进行选择，在年限下拉列表框中可以选择该域名购买年限，根据年限不同价格会有所差异，页面下侧推荐了可以选择的优惠产品，可以单击【加入购物车】按钮使用这些优惠产品，全部设置完成后单击【立即结算】按钮，如图 11-5 所示。

06 打开【核对确认订单信息】页面，需要在该页面填入申请人或企业的相关信息，信息录入要准确，配置完成后单击【确认订单，继续下一步】按钮，如图 11-6 所示。



图 11-5　购物车页面

31422221 您好！ [进入会员中心] [首页] [未付款订单] [在线提问] [退出]

万网 WWW.NET.CN

查看购物车 | 核对确认订单信息 | 选择支付方式 | 订单提交成功

请核对确认订单信息

域名所有人信息

域名所有者中文信息： ☑ 用会员信息自动填写
(如会员信息与域名所有者信息不符，请您仔细核对并修改)

域名所有者类型： 个人

域名所有者名称为业务重要标识，请填写与证件完全一致的名称

域名所有者名称： [redacted]

联系人： [redacted]

所属区域： 中国 河南 郑州市

通讯地址：

邮编：

联系电话： 86

传真号码： 86

电子邮箱： [redacted]

域名英文信息

国际通用顶级域名和国别域名所有者信息以英文信息为准，请不要缩写或简写信息

域名所有者名称（英文）：

联系人（英文）： 名 姓

省份（英文）： he nan

城市（英文）： zheng zhou shi

通信地址（英文）：

域名配置信息

域名密码： 请输入域名密码

选择域名解析服务器： ◉ 使用万网默认DNS服务器 ○ 自己设置DNS服务器

订单信息 [返回修改购物车]

产品名称	产品内容	年限	价格
.com英文域名	yinhangit.com	1年	139元 省 0元

结算信息

[使用优惠券]

订单金额：139元 - 优惠券：0 元 = **应付金额： 139元**
本次订单共省：0 元

☐ 我已阅读，理解并接受 [国际英文域名（.com）在线服务条款]

确认订单，继续下一步

关于我们 | 招贤纳士 | 友情链接 | 网站地图 | 公司位置 | 联系我们 | 万网公益 | 分销商专区

增值电信业务经营许可证（全国）（北京）备案确认书 电信与信息服务业务经营许可证 京ICP证050062号 电信业务审批[2005]字第194号 ISO9001国际标准质量体系认证
中国万网旗下网站：中国万网 第一指南 淘里淘外 移动万网 狼烟科技 通用网址：万网 中国万网 中文域名：万网.cn 中国万网.cn
Copyright © 2011 中国万网 版权所有 12321垃圾信息举报中心 域名注册服务批文号 信部电函[2005]374号 工信部备案系统认证

图 11-6 【核对确认订单信息】页面

07 打开【选择支付方式】页面，根据个人情况进行选择，然后单击【立即支付】按钮，如图 11-7 所示。

图 11-7　【选择支付方式】页面

08 中间支付过程不作介绍，支付成功后打开如图 11-8 所示的页面，单击【确认】按钮。

09 刚注册的域名还不能使用，还需要提交申请人和企业的域名资料，打开万网个人账户【域名管理】页面，右侧显示账户已有域名，域名资料状态为【未提交】，单击【提交资料】链接，如图 11-9 所示。



图 11-8　支付成功确认页面



图 11-9　【域名管理】页面

10 打开【域名资料提交】页面，选择当前域名的类型，本实例采用【国际域名资料提交】，

单击【点击进入】按钮，如图 11-10 所示。



图 11-10　【域名资料提交】页面

11 选择要提交资料的域名，在页面下侧选中域名前的复选框，单击【提交资料】按钮，如图 11-11 所示。



图 11-11　选择要提交资料的域名

12 打开【域名资料提交】页面，输入域名所有者、联系人信息，选择用户类型，如果选中【企业用户】单选按钮，需要提交企业有效营业执照的扫描副本及注册域名联系人的身份证明文件

扫描副本，资料上传之后单击【提交】按钮，如图 11-12 所示。



图 11-12 提交域名资料

13 域名资料上传成功，如图 11-13 所示。



图 11-13 域名资料提交成功

11.1.3 管理域名

域名申请成功后，需要对域名进行配置、管理，使其应用于网站发布。管理域名的具体内容如下。

01 使用万网会员账号登录，在左侧选项列表中选择【域名管理】选项，右侧显示了已申请的域名列表，如果域名比较多，可以通过【域名搜索】模块快速找到需要管理的域名，在下面域名列表中选择需要管理的域名，然后单击下面的一排管理按钮，可以实现各种管理功能，同时也可以单击域名列表后的【管理】链接，进入【域名基本信息】页面，如图 11-14 所示。



图 11-14　选择需要管理的域名

02 单击【管理】链接后，打开【域名基本信息】页面，显示了域名的基本信息，可以通过相关链接更改域名配置。域名最主要的功能是及时提供 Web 服务器的域名解析，单击【域名解析】链接，如图 11-15 所示。



图 11-15　【域名基本信息】页面

03 打开【域名解析】配置页面，在【便捷主机域名解析】文本框中输入 Web 服务器的 IP 地址，单击【新增】按钮，下面【域名解析记录】中显示了新增的两个主机记录（类型为 A 的记录），可以单击【修改】链接对其配置，如图 11-16 所示。



图 11-16　添加域名主机解析记录

至此，域名的注册和解析配置基本配置完成，已经可以满足 Web 服务器发布的使用，有关域名管理的其他配置不作过多介绍。

11.2　虚拟空间申请

中小企业通常使用的互联网接入方法是网通或电信的单线接入，且带宽资源有限。在这样的环境下对互联网发布企业服务器会影响服务器的访问效果，为了更好地为互联网用户提供访问效果，可以将企业对外发布服务器放置到专业的服务器发布环境中。IDC 机房就是提供这种业务需求的环境，IDC 机房称为互联网数据中心，可以提供各种互联网访问的增值服务。需要发布服务器的企业，可以从 IDC 机房租用服务器主机或者一部分虚拟空间来完成自己的发布需求。

本节将介绍虚拟主机的选择方法及其申请过程。

11.2.1　虚拟空间和虚拟主机的选择

企业发布服务器一般有两种选择，一种是租用虚拟主机，一种是租用虚拟空间。虚拟主机对于企业来说，就像是远端的一台计算机一样，管理员可以像远程登录计算机一样管理虚拟主机，它

可以提供更多的互联网服务，稳定性、性能等方面都有很好的保障。虚拟空间对于企业来说就像是存放在远程的一个 FTP 目录一样，管理员只要把自身的 Web 网站内容上传到虚拟空间的目录即可实现发布，不需要配置 IIS 或者 Apache 等发布环境。

虚拟空间的选择和域名的选择一样，都是服务器发布中的重要环节。虚拟主机的好与坏直接会影响企业服务的访问效果，如果选择的虚拟主机速度不行，客户访问时可能会延迟较长时间，影响企业形象。

下面分别介绍虚拟空间和虚拟主机的选择原则。

1. 选择虚拟空间

选择虚拟空间主要需要考虑一下要点。

（1）空间大小要能够满足当前网站文件的大小需求，不易过大，因为空间的增加会直接影响资金的投入，100M 的空间一年要 200~400 元/年，而 1G 的空间至少要 1000 元/年。但是空间也不易过于严格，要尽量留有一定的可扩充空间。

（2）编译网站的语言有很多，不同的网站使用的数据库也会有差异，对此空间也进行了分类。例如，用 PHP+MySQL 编写的网站，就必须要租用支持 PHP 和 MySQL 的空间，否则空间将发布失败。

（3）空间一般都会提供几个重要参数，访问连接数、每月流量、是否双线出口等。连接数限制了可同时访问网站的客户端数量，每月流量限制了一个月内可供访问下载的流量总数，而双线出口限制了该网站通过网通还是电信，或者两个运营商网络同时发布。以上配置内容影响了网站的访问效果，要结合自身需求进行选择。

2. 选择虚拟主机

选择虚拟主机的很多注意内容和选择虚拟空间是相似的。不过虚拟主机可以配置自己的发布环境，对于语言和发布程序没有太大的限制。管理员可以自己连接配置各种语言和数据库的发布环境，也可以选择使用 IIS 发布或者 Apache 发布服务器。

在选择虚拟主机的时候如果企业服务器对安全性和稳定性的要求比较高，可以考虑使用独立的虚拟主机。独立的虚拟主机相当于单独租用了一台硬件服务器，而普通的虚拟主机往往是使用虚拟技术将一台服务器设备虚拟成多个系统，分别租用给多个用户使用。相对来说，独立虚拟主机的安全性和稳定性较高。



提 示

目前有很多网站提供 1G 免费空间的申请，这些空间提供的虽然是 1G 的，但是这些空间的所提供的访问连接数和每月流量都比较低，并且没有很好的售后维护。一般个人网站可以使用，但是企业网站不建议使用。

11.2.2 申请虚拟主机

申请虚拟主机的方法和申请域名的方法相似。选择好合适的虚拟主机配置后，可以通过万网，或者当地的 IDC 托管机房申请获取虚拟主机。本书不详细介绍虚拟主机的申请过程。

11.3　管理企业服务器

虚拟主机或虚拟空间申请成功后，需要管理员进行管理和维护。虚拟主机一般使用远程桌面连接的方式进行管理，而虚拟空间一般使用 FTP 方式进行管理，具体操作方法介绍如下。

11.3.1　项目实战 2：使用远程桌面管理服务器

使用远程桌面管理的方式主要针对虚拟主机，这种管理方式很简单，具体操作步骤介绍如下。

01 选择【开始】➢【运行】选项，打开【运行】对话框，在【打开】文本框中输入“mstsc”命令，单击【确定】按钮，如图 11-17 所示。

02 弹出【远程桌面连接】对话框，在【计算机】文本框中输入申请虚拟主机时获得的管理 IP，单击【连接】按钮，即可连接到远程虚拟主机，如图 11-18 所示。

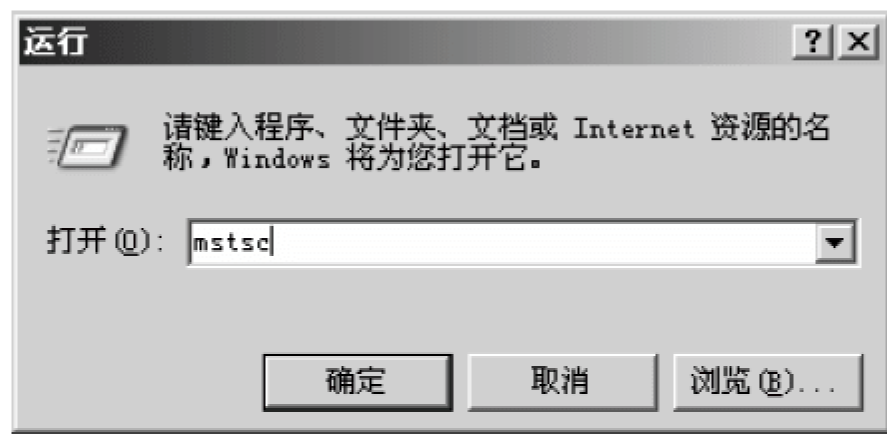


图 11-17　【运行】对话框

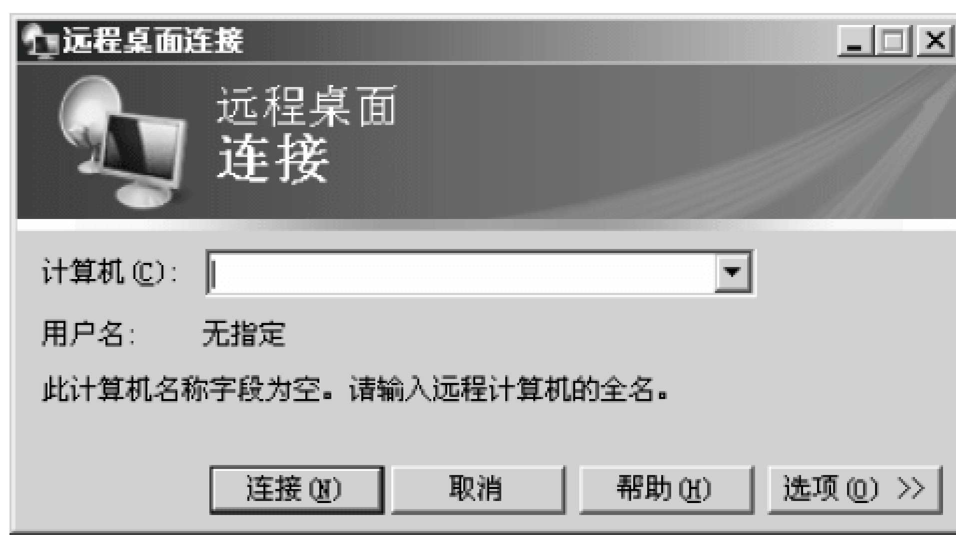


图 11-18　【远程桌面连接】对话框

连接时需要输入有权限的账户名及密码，管理员要妥善保管。

11.3.2　项目实战 3：使用 FTP 管理远程 Web 服务器

使用 FTP 的方式主要针对虚拟空间，操作方法也比较简单，可以通过 Windows 浏览器直接连接，也可以使用 FTP 客户端工具连接。本实例采用 6FTP 工具进行演示，具体操作步骤如下。

01 通过互联网获取 6FTP 程序，并安装在系统中。打开【6FTP 工具箱】窗口，如图 11-19 所示。

02 单击【站点设置】按钮，弹出【站点设置】对话框，在【站点名称】文本框中为该站点指定方便识别的站点名称，在【FTP 地址】文本框中输入虚拟空间的管理 IP 地址，在【用户名】和【密码】文本框中输入有权限的账户信息，FTP 服务端口为 21，所以【端口】文本框采用默认 21 端口，单击【增加新站点】按钮，如图 11-20 所示。

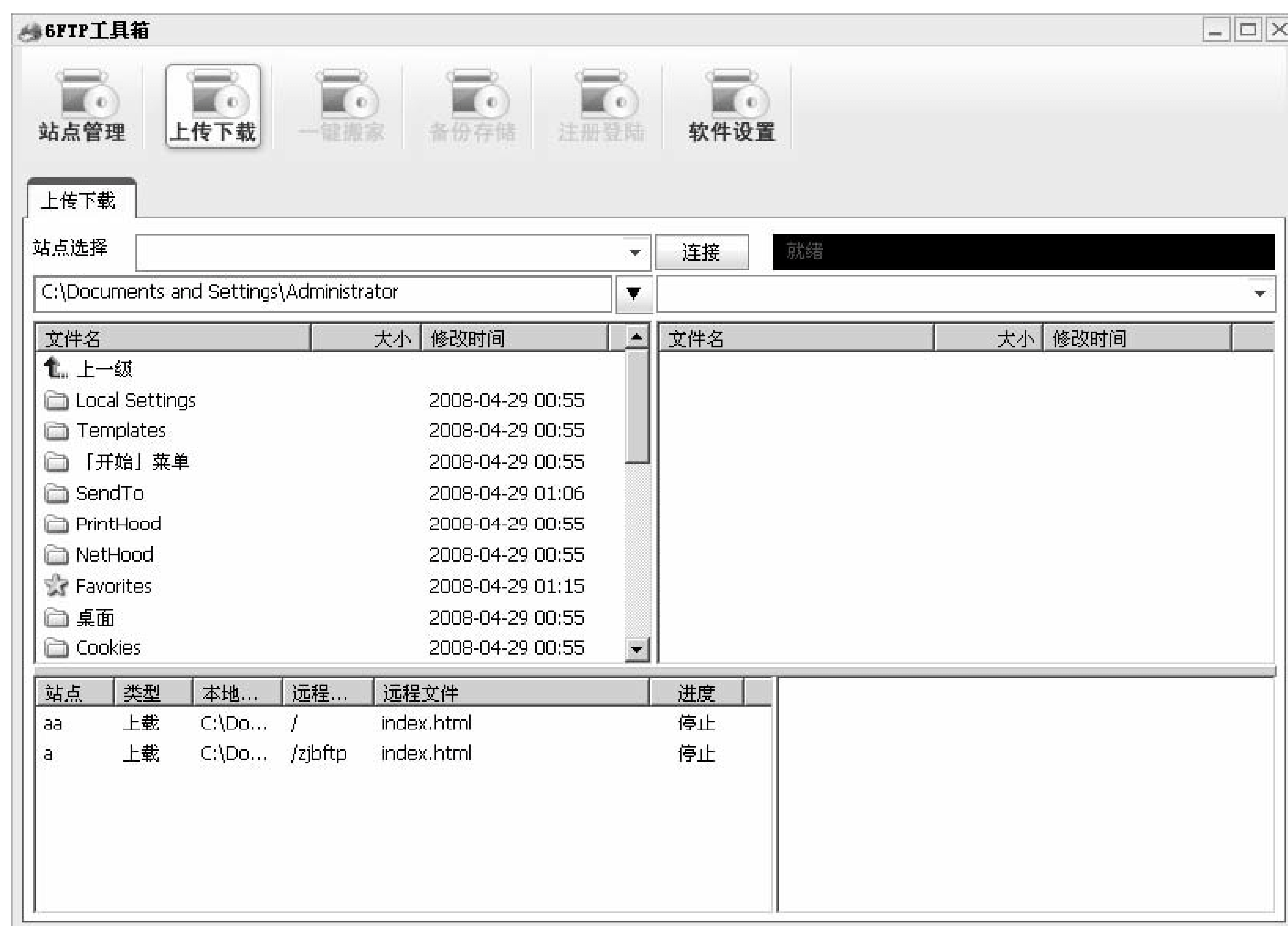


图 11-19　【6FTP 工具箱】窗口



图 11-20　【站点设置】对话框

03 添加站点成功后返回【6FTP 工具箱】窗口，在【站点选择】下拉列表框中选择新创建的站点“Web Server”，单击【连接】按钮，连接成功后可以右击左侧【文件名】列表中需要上传的文件或文件夹，在弹出的快捷菜单中选择【上传】命令，将其上传到目标虚拟空间的目录中，如图 11-21 所示。

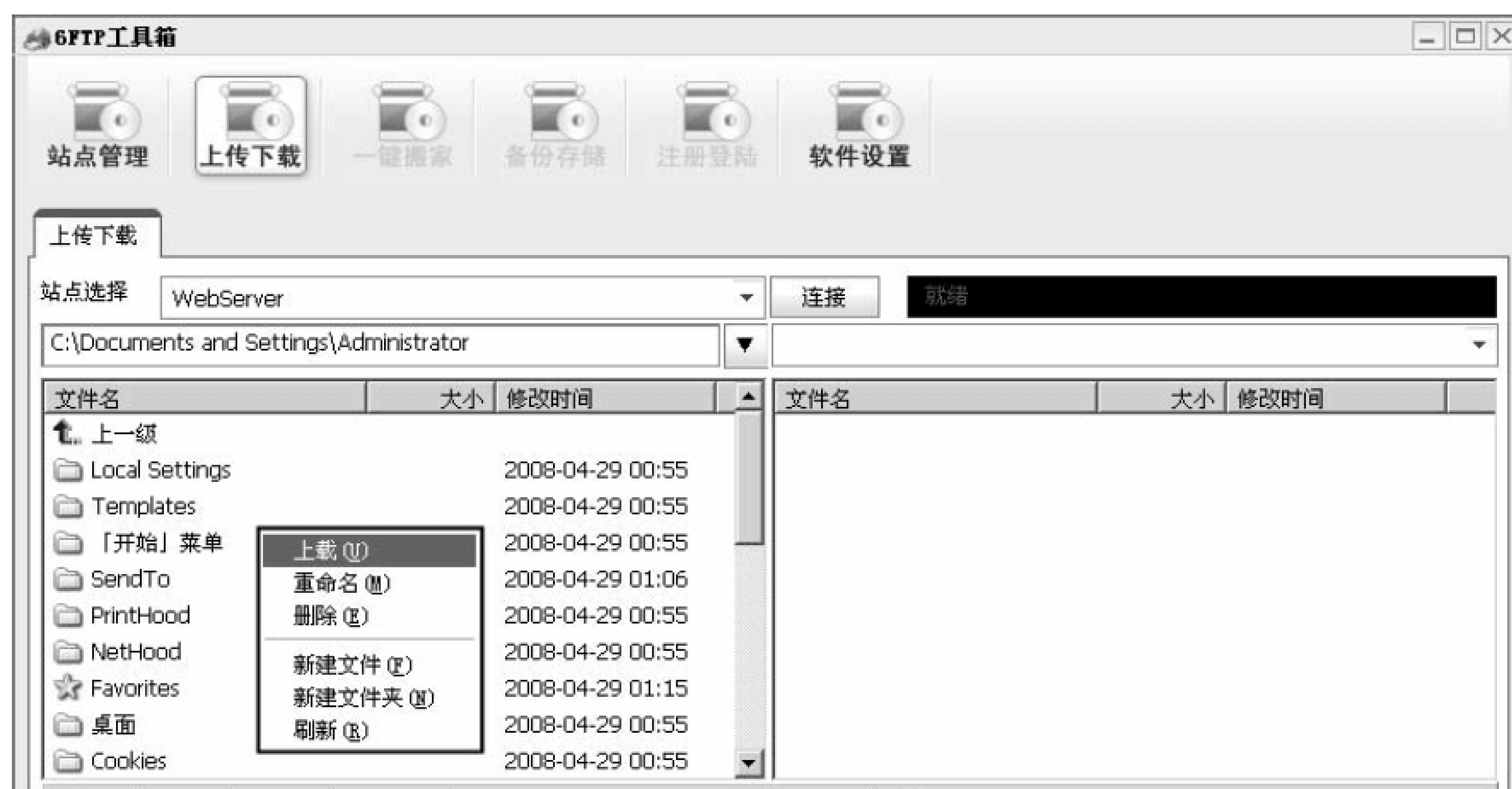


图 11-21 连接站点

11.4 专家答疑

（1）申请的虚拟主机是否能够保证数据安全呢？

答：在网络中没有绝对的安全，但是在专业的服务器托管机房都会配置专门的安全设备，如防火墙、入侵检测系统等。而且这些服务器机房的整体环境是非常标准的，相对企业自己管理服务器来说会更加稳定。这样来看申请的虚拟主机是可以保证数据安全的。

但是，虚拟主机存在的机房可以被机房的管理人员接触到，可以被直接物理接触，再好的安全软件也会如同虚设，所以在使用虚拟主机时要防备机房管理人员的拷贝，一般建议企业不要将重要的数据信息上传到服务器存放。

（2）申请空间或虚拟主机时是申请国外的服务器好，还是国内的好？

答：国内外的服务器各有优势，需要看空间的使用需求。

如果申请的空间主要用于国内用户访问，则建议使用国内的服务器，因为申请国外服务器的话，国内用户访问时需要首先从国内网络出口出去到达国外网络，而整个国家的网络出口是比较有限的，所以选择国外服务器的话会严重影响国内用户的访问速度。而且国内服务器在相对于国内企业来说更利于售后管理。

第 12 章　企业网络存储服务管理与维护

对于很多企业来说，网络环境中最重要的不是设备，而是整个网络运作产生的数据和整个企业业务相关的信息。本章将详细介绍用于存储、管理这些数据信息的网络存储服务器的相关操作内容。

12.1　网络存储服务器概述

网络存储服务器，可以简单地认为是网络中主要提供存储的服务器。典型的服务器会被配置实现诸如 Web 服务、应用数据库服务、打印服务等，这些服务器一般会配置较高的处理器和内存，并连接一定的存储空间。但是存储服务器并不是这样，它的主要目的就是提供存储服务，对于一般的服务器来说连接 4~5 块硬盘已经算多了，而存储服务器连接的磁盘空间至少 6 块，甚至 12 块、24 块或 32 块。

一般的服务器使用磁盘时大都是直接连接使用，而存储服务器的磁盘并不是简单地连接到主机中，往往会采用专业的磁盘存放设备——磁盘阵列柜，大量的磁盘插入大磁盘阵列柜中，磁盘阵列柜相当于外接设备连接主机。

那么，除了提供大量的外接存储空间外，存储服务器还会携带很多的特殊服务，如专业的存储管理软件、多样灵活的 RAID 配置类型、友好的客户桌面连接端程序等。

12.2　项目实战 1：磁盘管理基础配置

存储服务器中管理最多的还是磁盘，对于网络管理员来说，需要熟练掌握磁盘的容错技术、配额配置、数据备份等内容。本节将对这些内容进行详细的讲解，具体内容如下。

12.2.1　使用 RAID 磁盘容错技术配置分区

RAID 磁盘容错技术是提高数据可靠性和读写速度的有效方法，下面详细介绍几种常见的 RAID 技术。

1. 挂载磁盘

在配置 RAID 磁盘容错之前，要首先挂载几块磁盘，而且这些磁盘要变为动态磁盘，具体操

作步骤如下。

01 在主机上连接 3 块硬盘，分别为 10G 大小，启动系统后打开【服务器管理器】窗口，在左侧列表中选择【存储】➢【磁盘管理】选项，在右侧显示了新连接的 3 块磁盘，如图 12-1 所示。

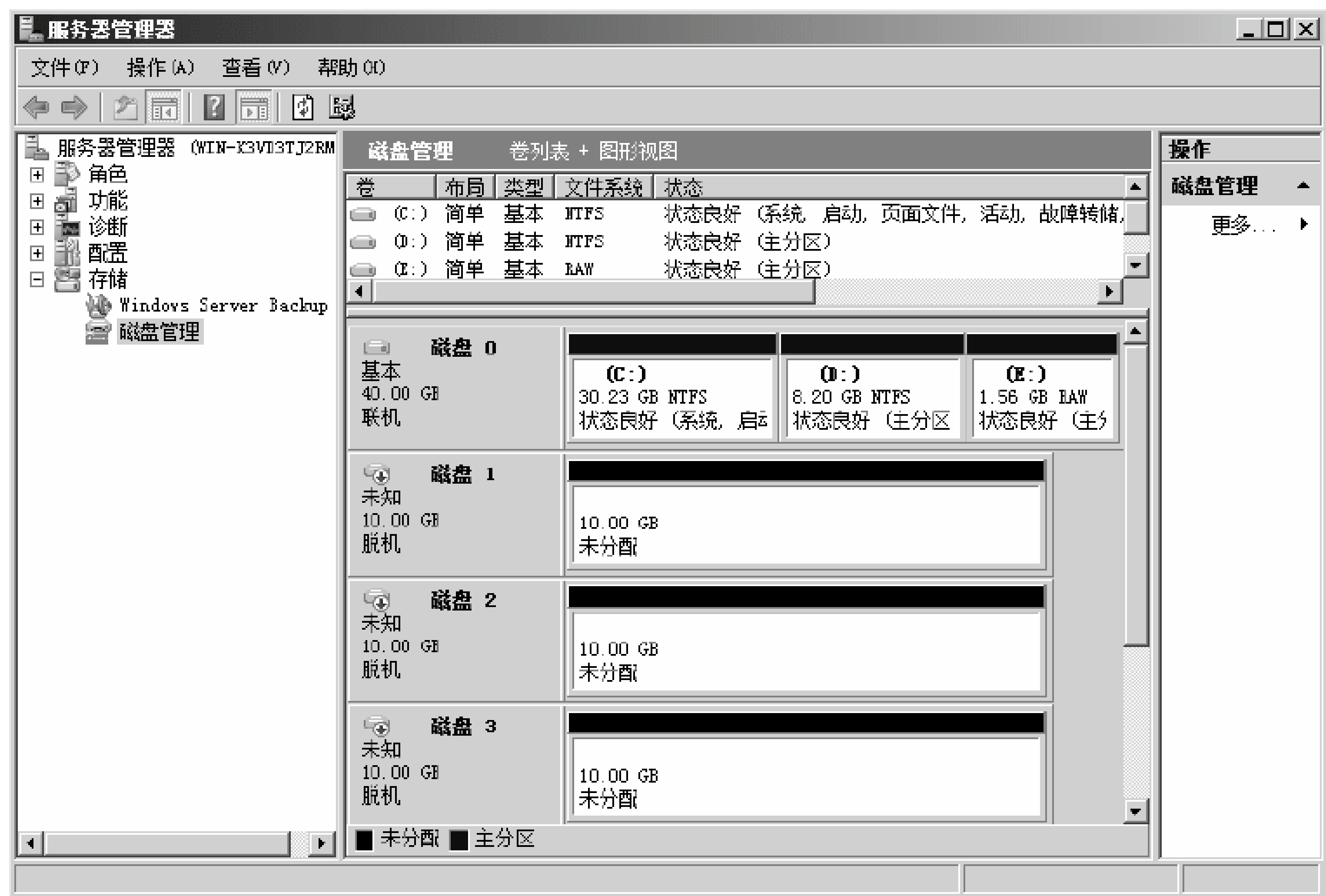


图 12-1 【服务器管理器】窗口

02 右击【磁盘 1】，在弹出的快捷菜单中选择【联机】命令，如图 12-2 所示。其他磁盘使用相同方法联机。



图 12-2 进行磁盘联机

03 联机完成后，显示磁盘没有初始化，右击磁盘，在弹出的快捷菜单中选择【初始化磁盘】命令，如图 12-3 所示。

04 弹出【初始化磁盘】对话框，选中需要初始化的三块磁盘名称前的复选框，磁盘分区形式采用默认选项 MBR，单击【确定】按钮，如图 12-4 所示。



图 12-3　进行磁盘初始化

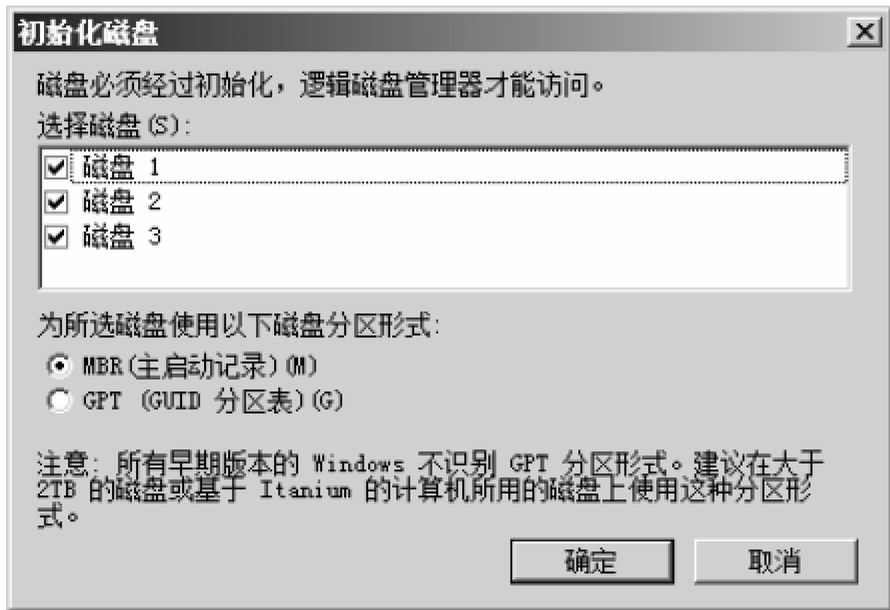


图 12-4　【初始化磁盘】对话框

05 三块磁盘初始化完成，显示为基本磁盘，一般 RAID 是在动态磁盘基础上配置的，所以右击磁盘，在弹出的快捷菜单中选择【转换到动态磁盘】命令，如图 12-5 所示。

06 弹出【转换为动态磁盘】对话框，选择需要转换为动态磁盘的三块新加磁盘，单击【确定】按钮，如图 12-6 所示。一般系统所在磁盘在转换为动态磁盘时需要重启系统。



图 12-5　将磁盘转换为动态磁盘

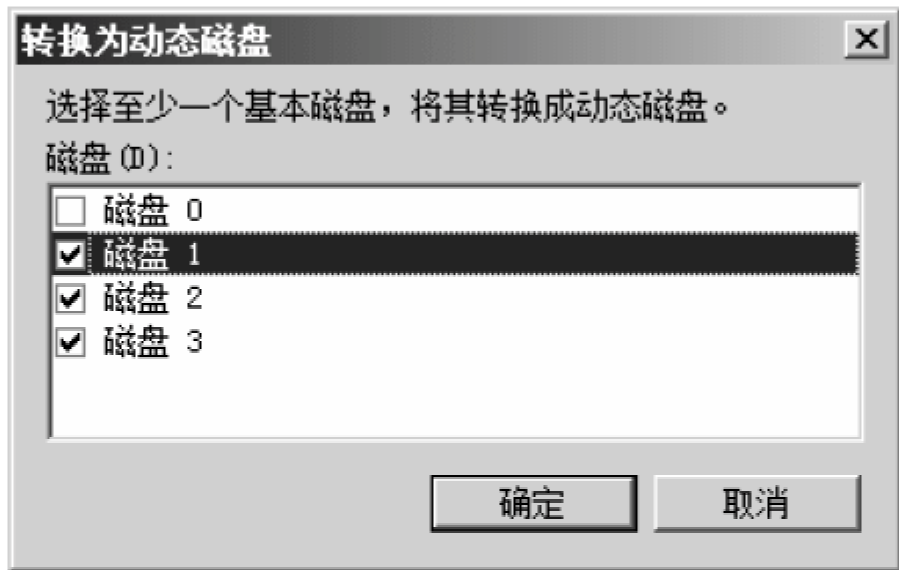


图 12-6　【转换为动态磁盘】对话框

2. 新建简单卷

所谓简单卷，是在动态磁盘中最普通的分区，和通常磁盘分区中的分区相似。新建简单卷的具体操作步骤如下。

01 右击磁盘空间，在弹出的快捷菜单中选择【新建简单卷】命令，如图 12-7 所示。



图 12-7　新建简单卷

02 弹出【新建简单卷向导】对话框，单击【下一步】按钮，如图 12-8 所示。

03 弹出【指定卷大小】对话框，在【简单卷大小（MB）】文本框中输入需要创建的分区大小，本实例为 5120MB，单击【下一步】按钮，如图 12-9 所示。

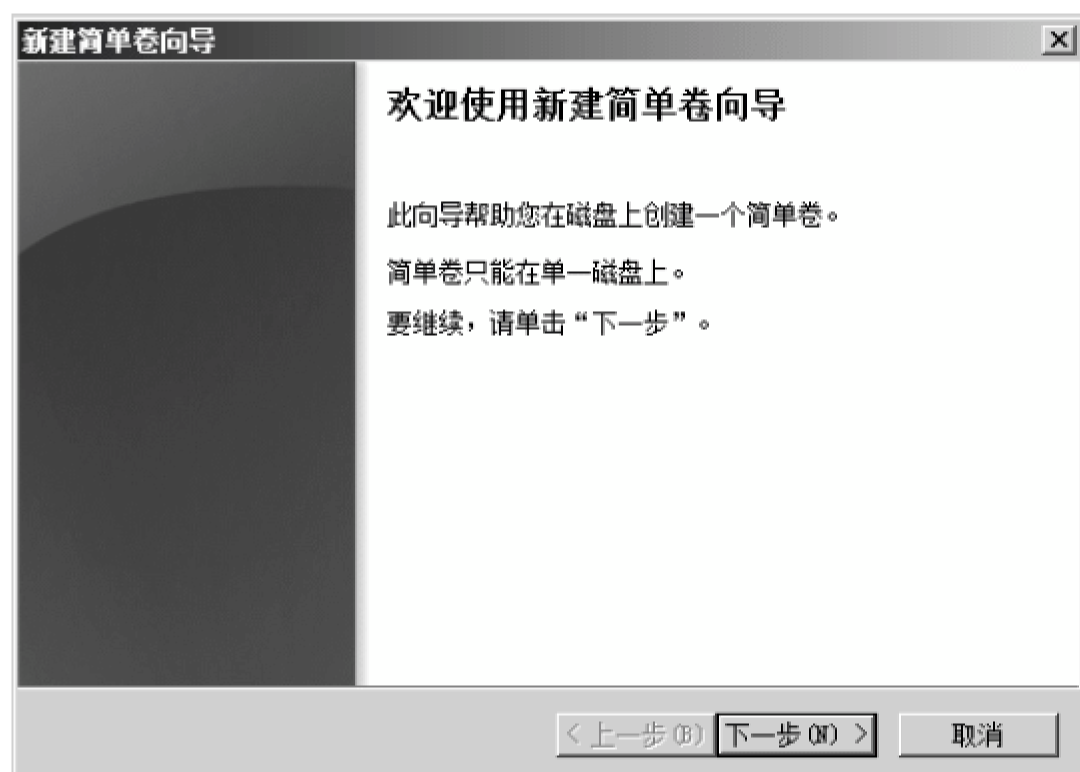


图 12-8 【新建简单卷向导】对话框



图 12-9 【指定卷大小】对话框

04 弹出【分配驱动器号和路径】对话框，选中【分配以下驱动器号】单选按钮，在后面的下拉列表框中选择合适的盘符号，单击【下一步】按钮，如图 12-10 所示。

05 弹出【格式化分区】对话框，选择【按下列设置格式化这个卷】单选按钮，在【文件系统】下拉列表框中选择 NTFS 文件系统类型，在【分配单元大小】下拉列表框中选择【默认值】，即 1024 字节为单位格式化卷，【卷标】文本框可根据需求自行定义，选中【启用文件和文件夹压缩】复选框可以使该卷存储的所有文件都执行默认压缩，以节省空间。配置完成后，单击【下一步】按钮，如图 12-11 所示。

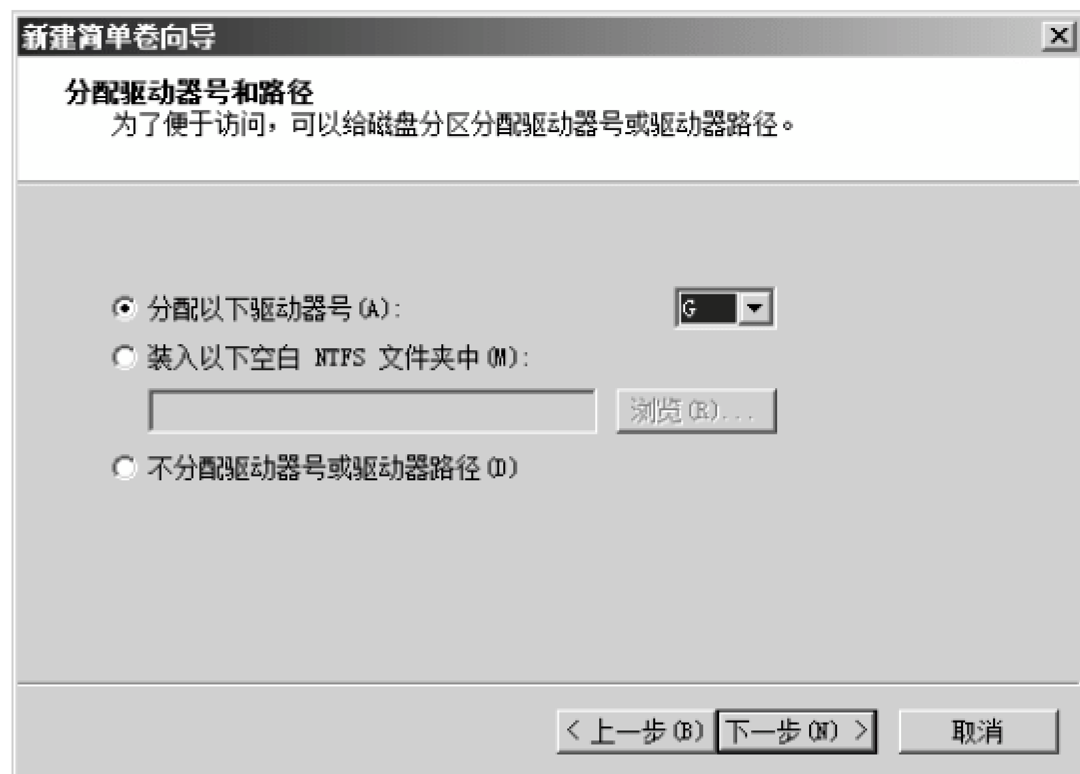


图 12-10 【分配驱动器号和路径】对话框

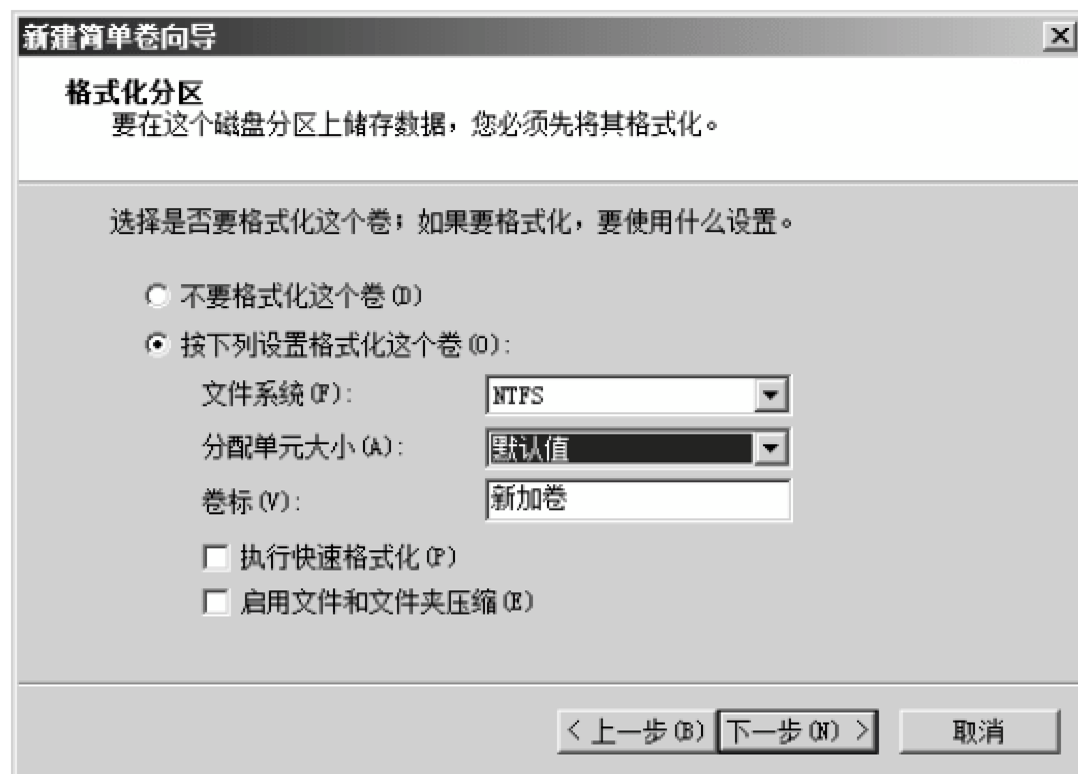


图 12-11 【格式化分区】对话框

06 弹出【正在完成新建简单卷向导】对话框，显示配置信息，单击【完成】按钮，如图 12-12 所示。

07 返回磁盘管理列表，新卷已经创建成功，并显示为棕色，如图 12-13 所示。

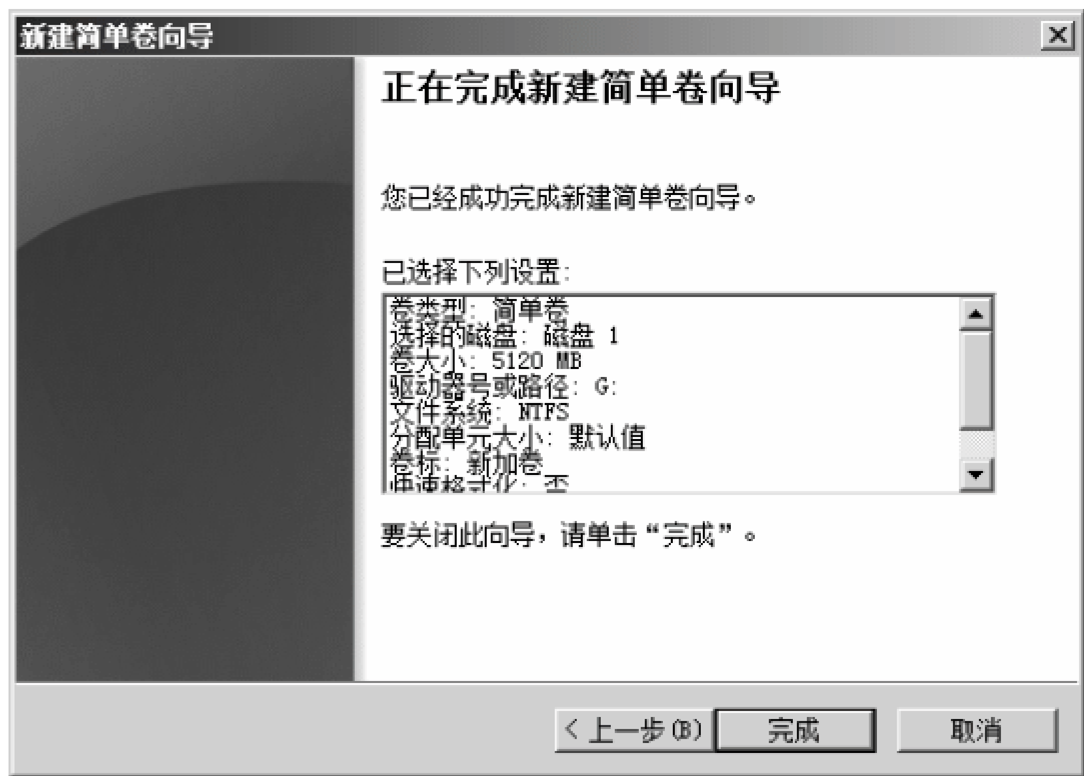


图 12-12 【正在完成新建简单卷向导】对话框

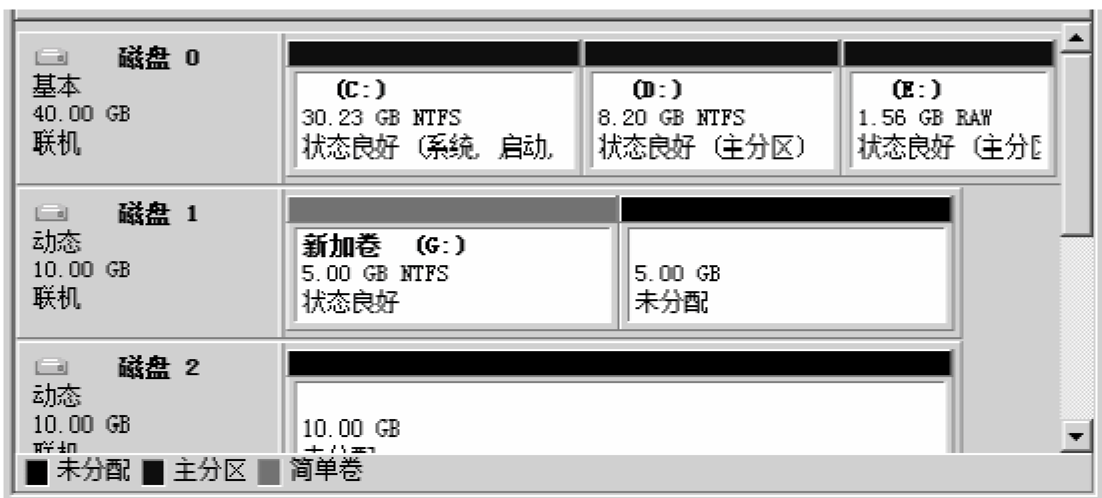


图 12-13 新卷创建成功

3. 新建跨区卷

在普通的基本磁盘中一个分区不可能跨越两块磁盘，而动态磁盘可以使用创建跨区卷的方法将两个磁盘的空间分配到同一个分区中。在单个磁盘剩余空间有限的情况下，可以使用这种方法将多个磁盘的剩余空间整合在一起使用。但是在存放数据的时候会先使用完一个磁盘上的部分空间，然后才会使用其他磁盘的空间，不能够提高读写速度。

创建跨区卷的具体操作步骤如下。

01 右击磁盘空间，在弹出的快捷菜单中选择【新建跨区卷】命令，如图 12-14 所示。



图 12-14 新建跨区卷

02 弹出【新建跨区卷】对话框，单击【下一步】按钮，如图 12-15 所示。

03 弹出【选择磁盘】对话框，可以选择左侧【可用】磁盘列表，通过单击【添加】按钮将其加入到右侧【已选的】磁盘列表中，选中已选磁盘可以在【选择空间量】文本框中输入创建的新分区从该磁盘调用的空间大小，两个磁盘上调用的空间可以不相同。配置完成后单击【下一步】按钮，如图 12-16 所示。

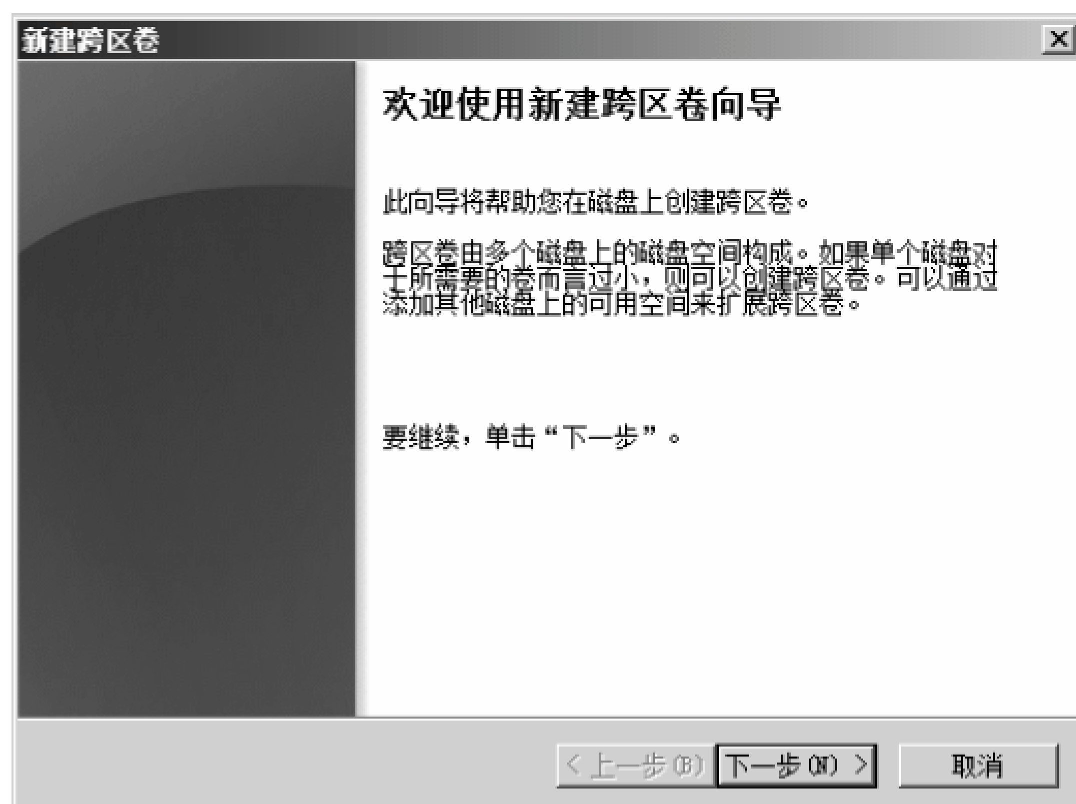


图 12-15 【新建跨区卷】对话框

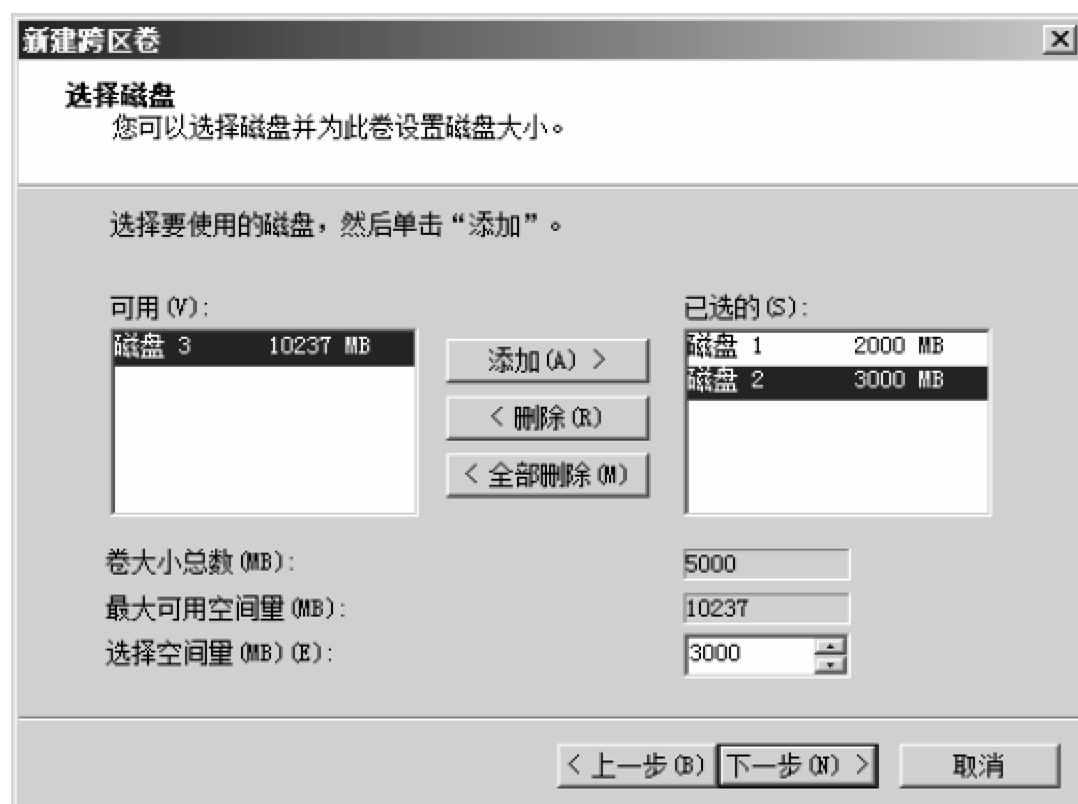


图 12-16 【选择磁盘】对话框

04 弹出【分配驱动器号和路径】对话框，选中【分配以下驱动器号】单选按钮，在后面的下拉列表框中选择合适的盘符号，单击【下一步】按钮，如图 12-17 所示。

05 弹出【格式化分区】对话框，选择【按下列设置格式化这个卷】单选按钮，其他采用默认配置，单击【下一步】按钮，如图 12-18 所示。

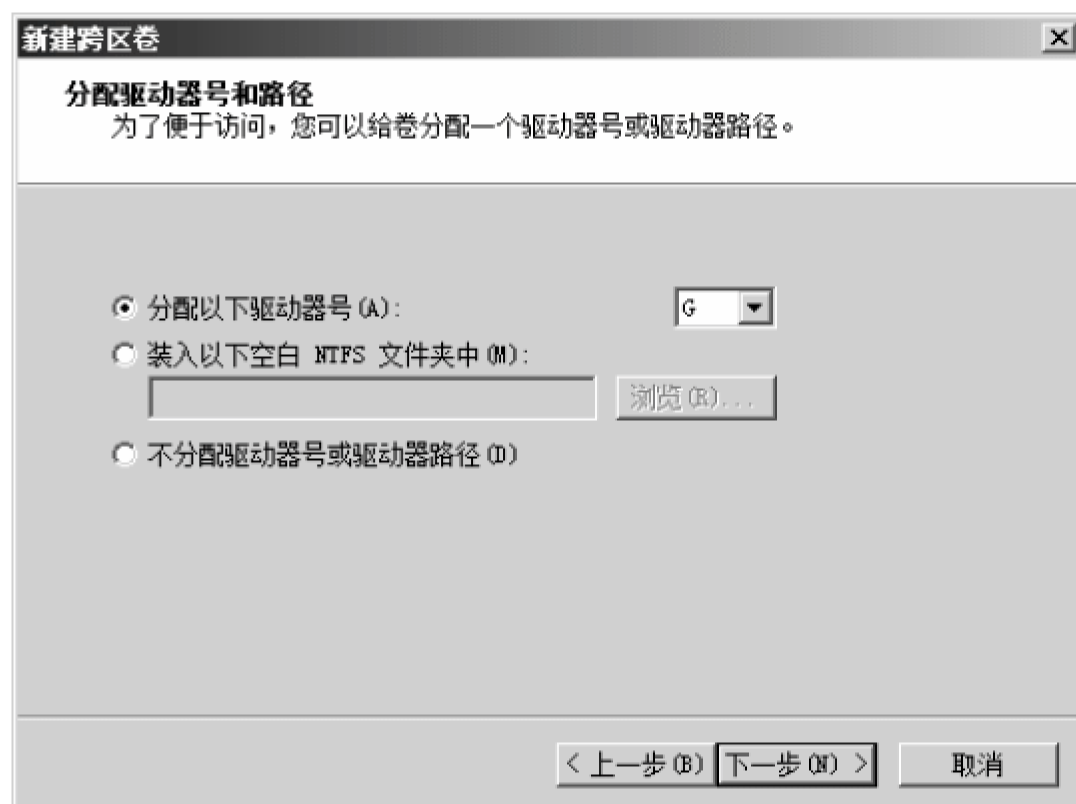


图 12-17 【分配驱动器号和路径】对话框

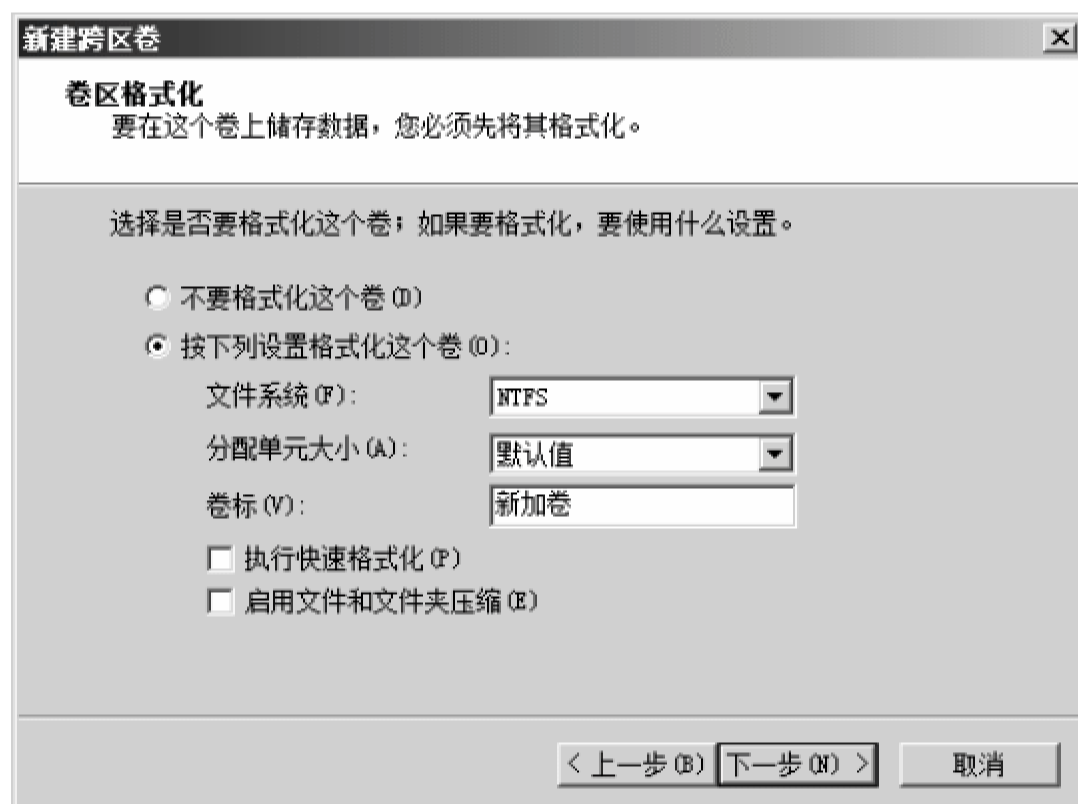


图 12-18 【卷区格式化】对话框

06 弹出【正在完成新建跨区卷向导】对话框，显示配置信息，单击【完成】按钮，如图 12-19 所示。

07 返回磁盘管理列表，新的跨区卷已经创建成功，并显示为紫色，如图 12-20 所示。

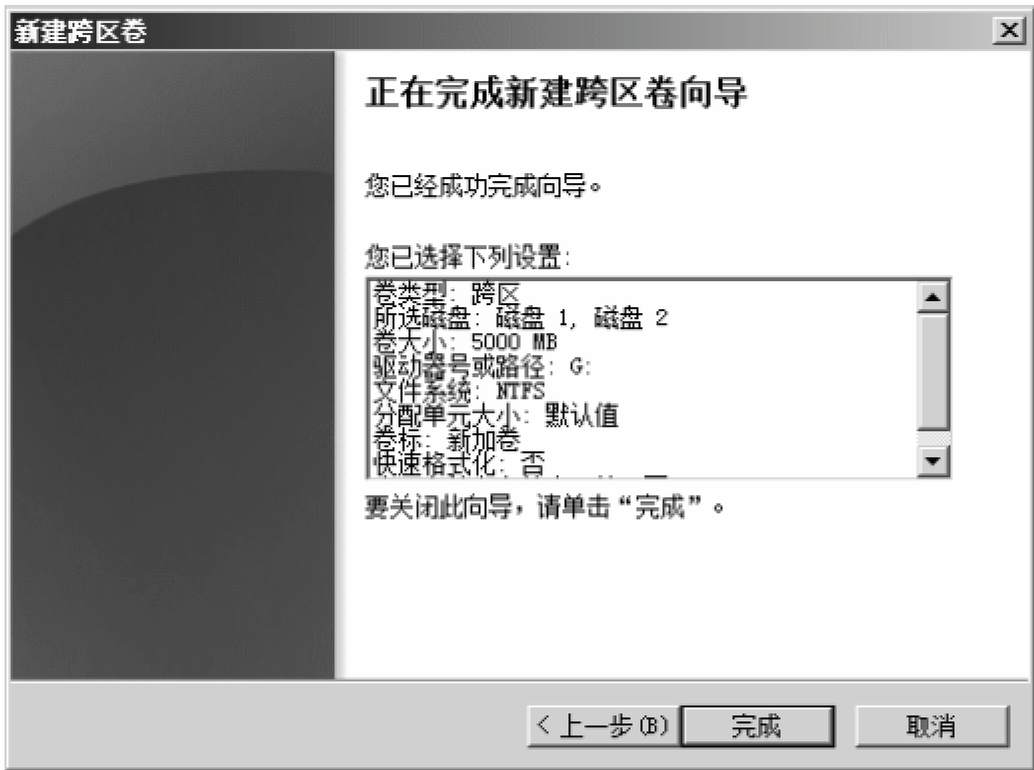


图 12-19　【正在完成新建跨区卷向导】对话框



图 12-20　跨区卷创建成功

4. 新建带区卷

带区卷和跨区卷相似，可以创建一个同时跨越多个磁盘的卷，但是不同的是带区卷从每一个磁盘上调用的空间要完全相同。数据写入时，会将数据分割成单位大小，并将这些单位大小的数据逐一在每一个创建带区卷的磁盘上存放，读取时也会向每个磁盘逐一请求读取，这样可以造成多个磁盘同时读写的现象，可以大大提高读写速度。

新建带区卷的具体操作步骤如下。

01 右击磁盘空间，在弹出的快捷菜单中选择【新建带区卷】命令，如图 12-21 所示。



图 12-21　新建带区卷

02 弹出【新建带区卷】对话框，单击【下一步】按钮，如图 12-22 所示。

03 弹出【选择磁盘】对话框，可以选择左侧【可用】磁盘列表，通过单击【添加】按钮将其加入到右侧【已选的】磁盘列表中，选中已选磁盘可以在【选择空间量】文本框中输入创建的新分区从该磁盘调用的空间大小，所有已选磁盘会调用相同大小的空间。配置完成后单击【下一步】按钮，如图 12-23 所示。

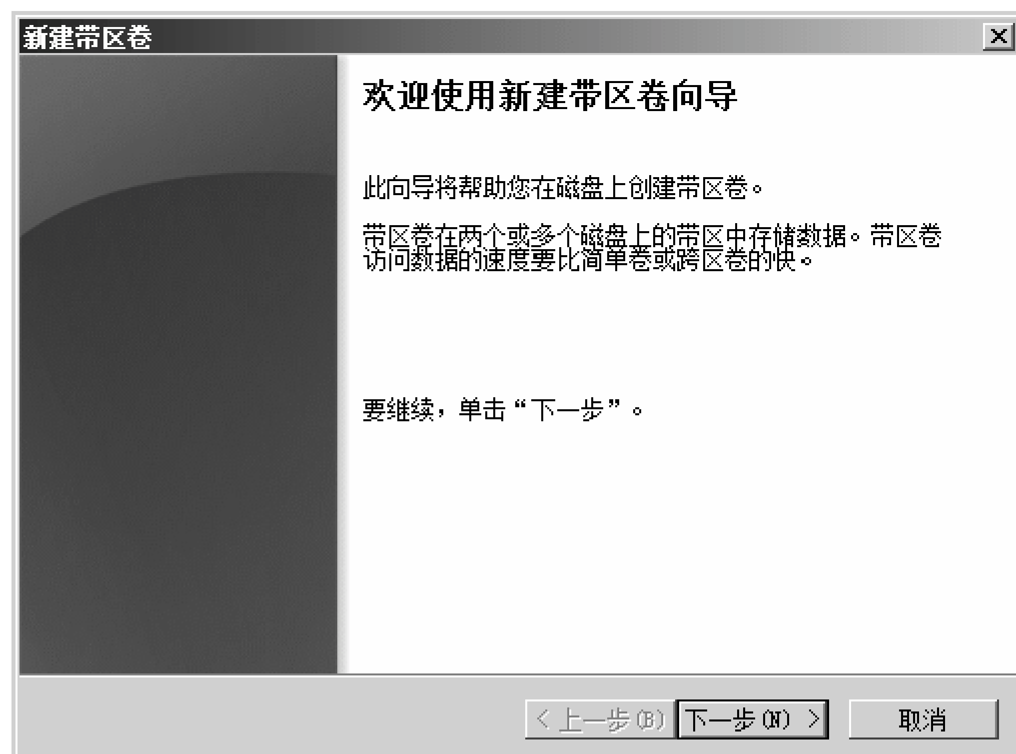


图 12-22 【新建带区卷】对话框



图 12-23 【选择磁盘】对话框

04 弹出【分配驱动器号和路径】对话框，选中【分配以下驱动器号】单选按钮，在后面的下拉列表框中选择合适的盘符号，单击【下一步】按钮，如图 12-24 所示。

05 弹出【卷区格式化】对话框，选中【按下列设置格式化这个卷】单选按钮，其他采用默认配置，单击【下一步】按钮，如图 12-25 所示。

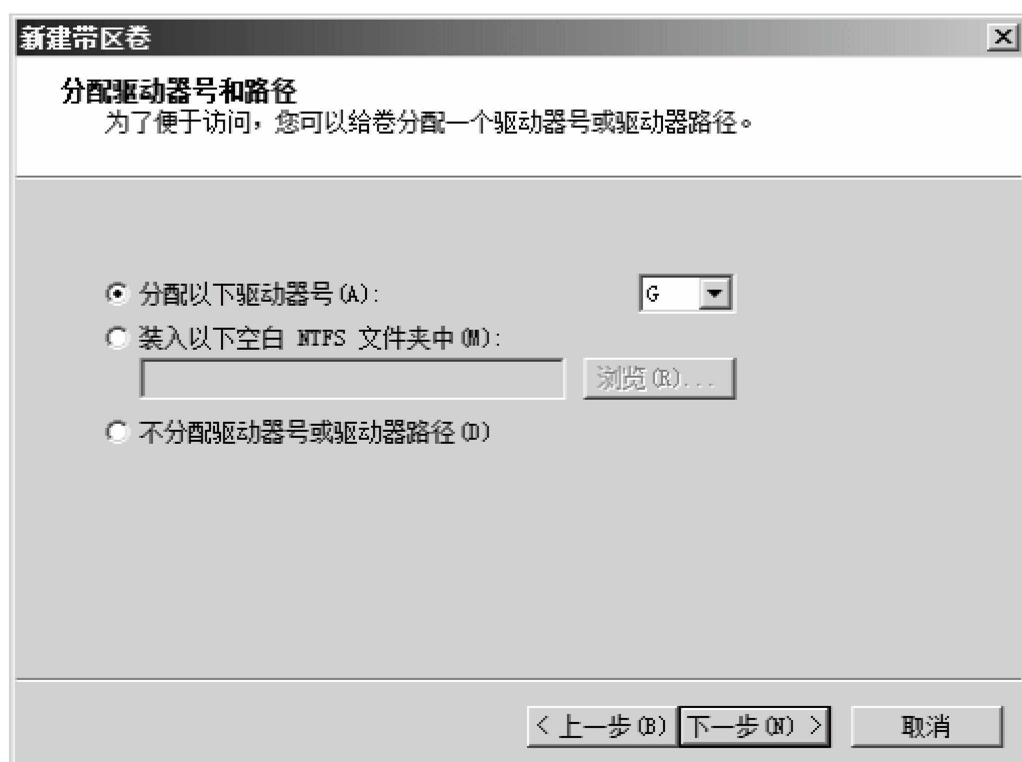


图 12-24 【分配驱动器号和路径】对话框

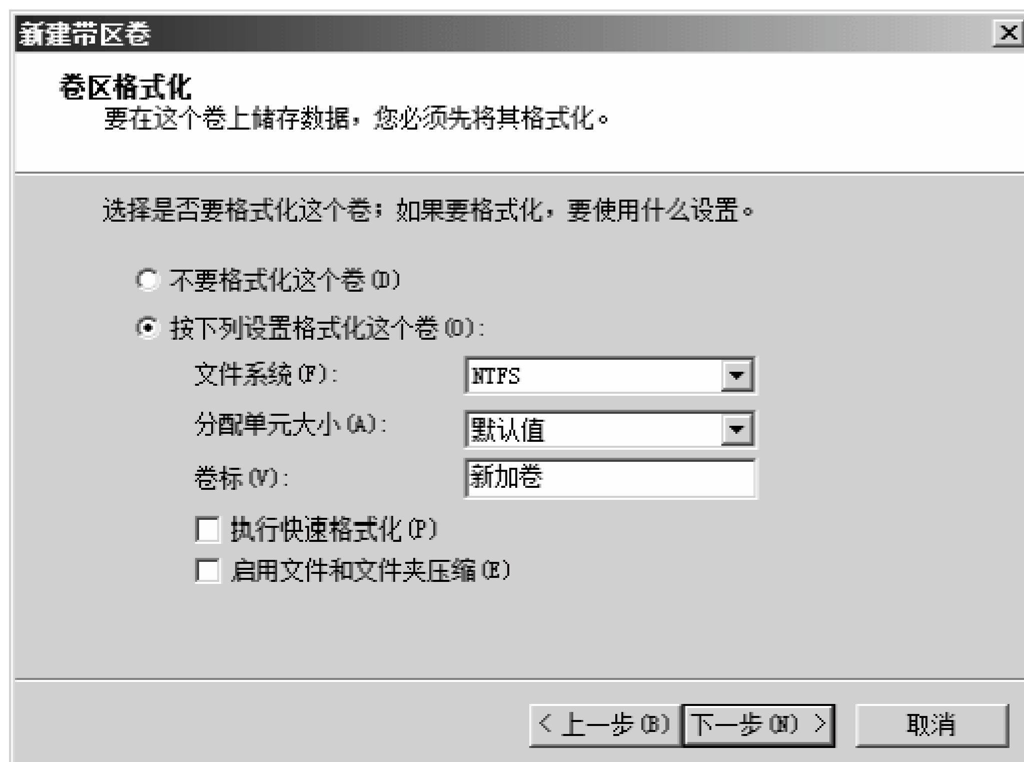


图 12-25 【卷区格式化】对话框

06 弹出【正在完成新建带区卷向导】对话框，显示配置信息，单击【完成】按钮，如图 12-26 所示。

07 返回磁盘管理列表，新卷已经创建成功，并显示为绿色，如图 12-27 所示。

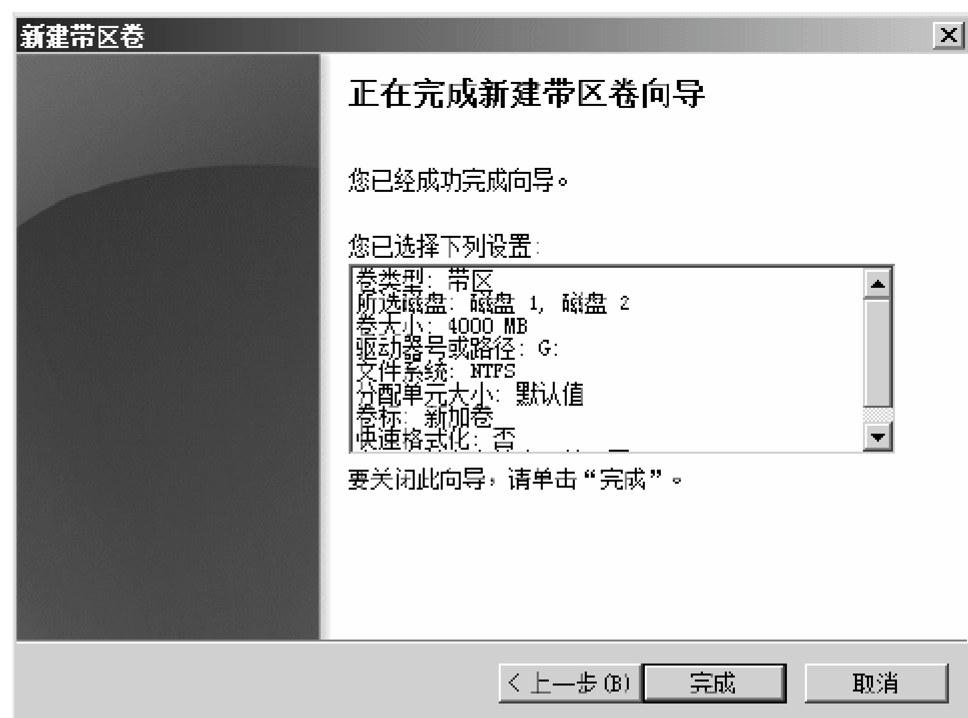


图 12-26 【正在完成新建带区卷向导】对话框



图 12-27 带区卷创建成功

5. 新建镜像卷

镜像卷是从两个磁盘中调用相同的空间互作镜像，即所有的数据在互为镜像卷的两个磁盘空间上同时存放。数据被存了两份，当一个磁盘被损坏后，另外一个磁盘还可以正常提供工作。镜像卷一般用于服务器的系统分区，这样可以确保系统可靠、持续地运行。需要说明的是，镜像卷并不能够提高读写速度。

新建镜像卷的具体操作步骤如下。

01 右击磁盘空间，在弹出的快捷菜单中选择【新建镜像卷】命令，如图 12-28 所示。



图 12-28 新建镜像卷

02 弹出【新建镜像卷】对话框，单击【下一步】按钮，如图 12-29 所示。

03 弹出【选择磁盘】对话框，可以选择左侧【可用】磁盘列表，通过单击【添加】按钮将其加入到右侧【已选的】磁盘列表中，选中已选磁盘可以在【选择空间量】文本框中输入创建的新分区从该磁盘调用的空间大小，所选的两块磁盘会调用相同大小的空间。配置完成后单击【下一步】按钮，如图 12-30 所示。

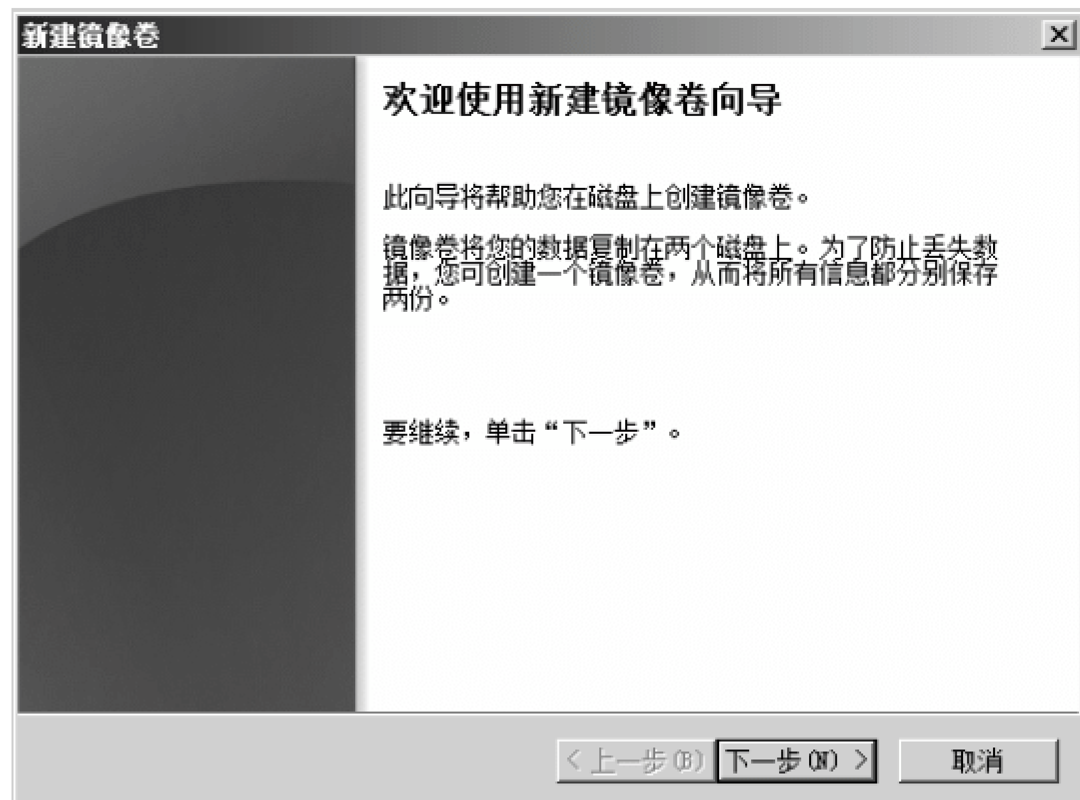


图 12-29 【新建镜像卷】对话框

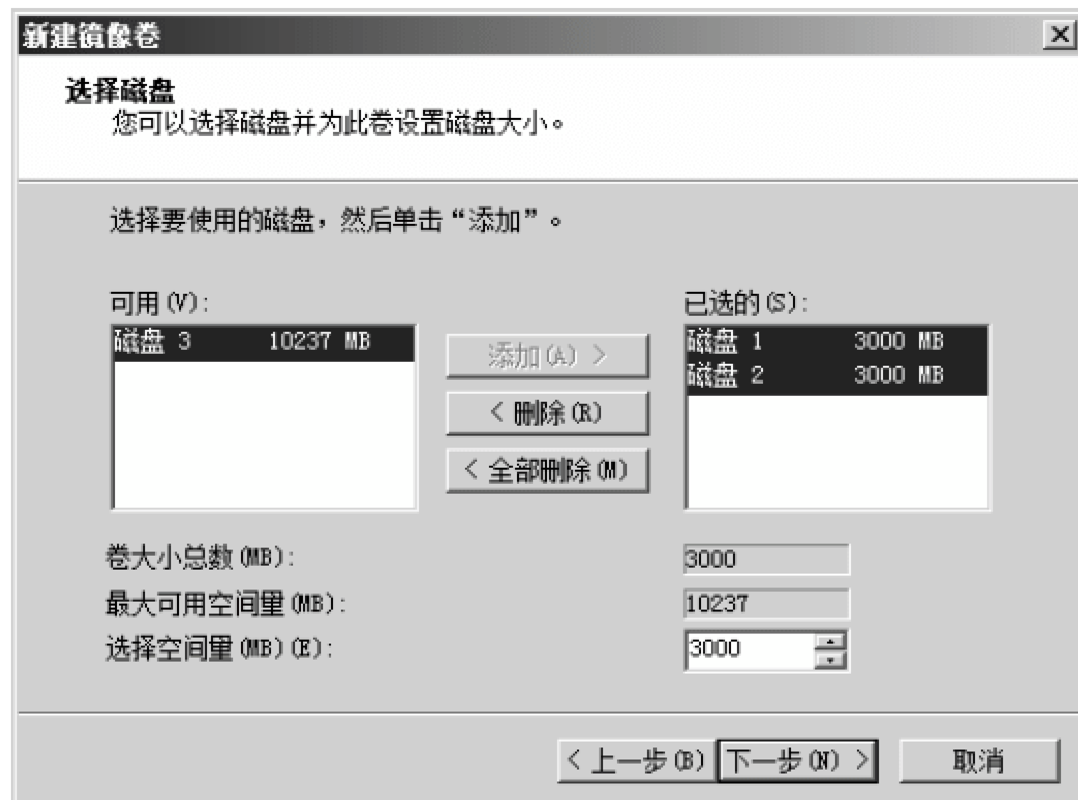


图 12-30 【选择磁盘】对话框

04 弹出【分配驱动器号和路径】对话框，选中【分配以下驱动器号】单选按钮，在后面的下拉列表框中选择合适的盘符号，单击【下一步】按钮，如图 12-31 所示。

05 弹出【卷区格式化】对话框，选中【按下列设置格式化这个卷】单选按钮，其他采用默认配置，单击【下一步】按钮，如图 12-32 所示。

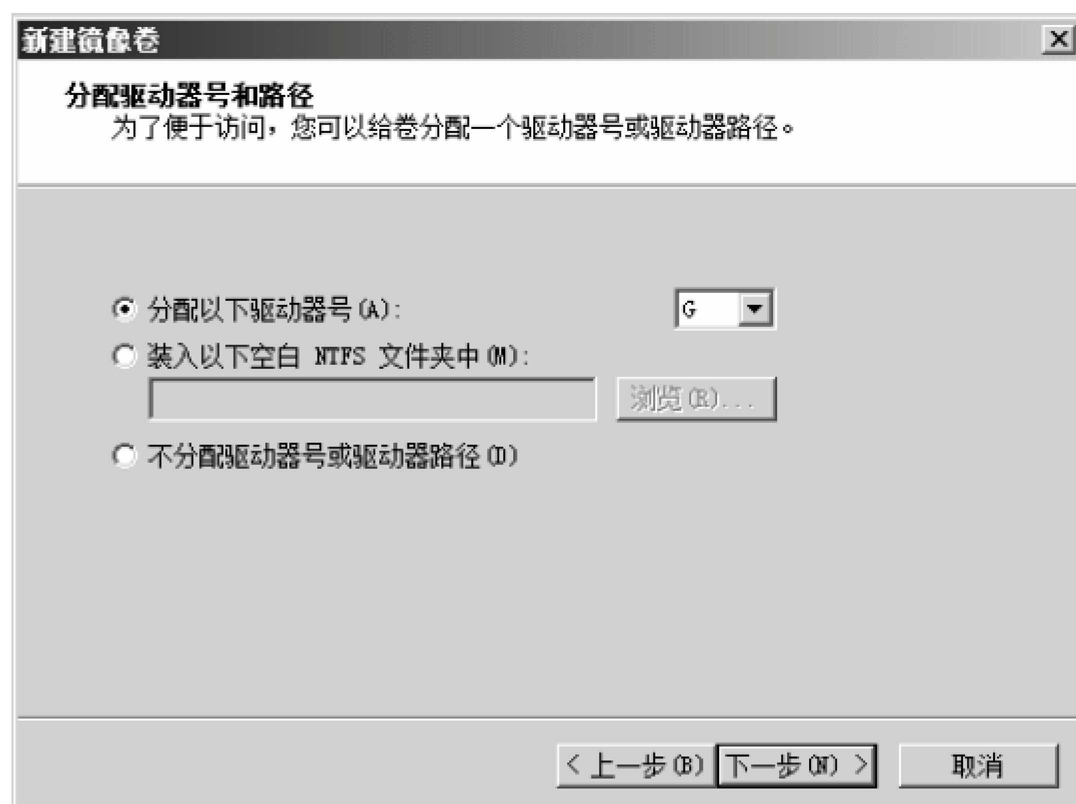


图 12-31 【分配驱动器号和路径】对话框

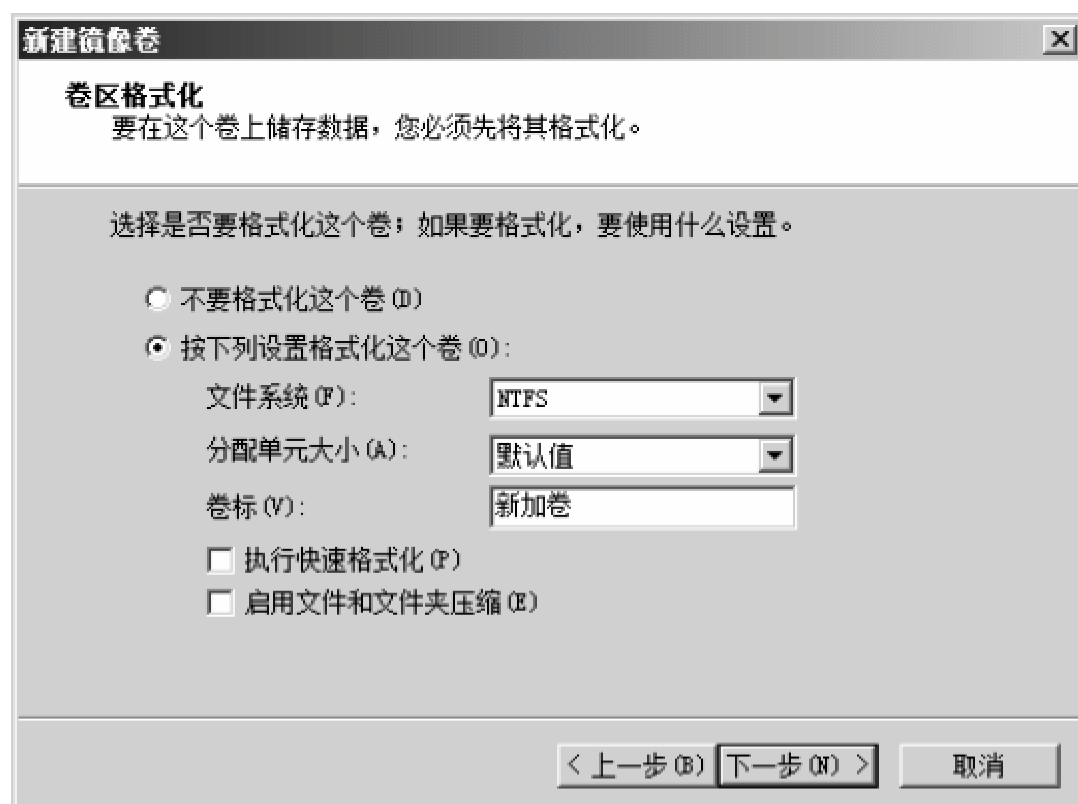


图 12-32 【卷区格式化】对话框

06 弹出【正在完成新建镜像卷向导】对话框，显示配置信息，单击【完成】按钮，如图 12-33 所示。

07 返回磁盘管理列表，新的镜像卷已经创建成功，并显示为红色，如图 12-34 所示。

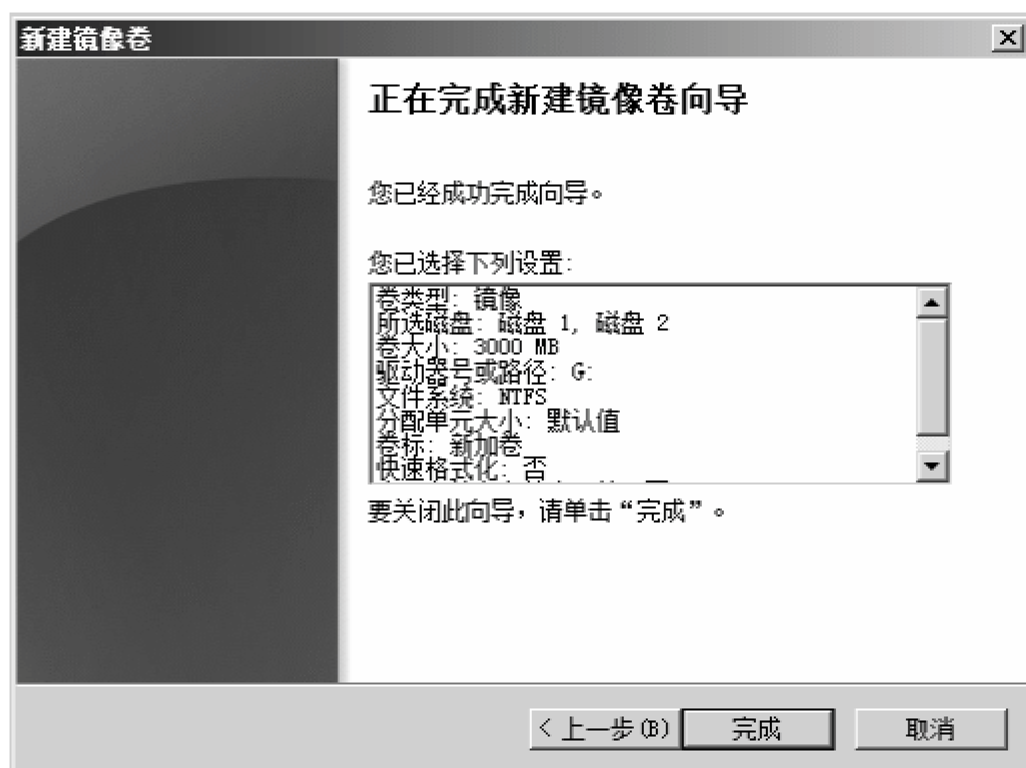


图 12-33 【正在完成新建镜像卷向导】对话框



图 12-34 镜像卷创建成功

6. 新建 RAID-5 卷

RAID-5 卷是从三块以上的磁盘中调用相同的空间创建的卷，在进行数据存储时会拿出一个磁盘的空间对其他磁盘空间中的数据做校验。例如，从三个磁盘中分别调用 10G 空间做一个 RAID-5 卷，其中一个磁盘会将另外两个磁盘中的数据做校验运算，并保存校验值。当构成 RAID-5 卷的多个磁盘中有一个磁盘损坏时，可以通过其他磁盘的数据或者校验值将这个磁盘原有的数据恢复。

RAID-5 卷具有很好的数据冗余性，而且只拿出来 1/N（N 表示构成 RAID-5 卷的磁盘数量）的空间做冗余校验，不像镜像卷那样浪费空间，又由于多个磁盘同时读写而提高了效率。

新建 RAID-5 卷的具体操作步骤如下。

01 右击磁盘空间，在弹出的快捷菜单中选择【新建 RAID-5 卷】命令，如图 12-35 所示。



图 12-35　新建 RAID-5 卷

02 弹出【新建 RAID-5 卷】对话框，单击【下一步】按钮，如图 12-36 所示。

03 弹出【选择磁盘】对话框，可以选择左侧【可用】磁盘列表，通过单击【添加】按钮将其加入到右侧【已选的】磁盘列表中，至少添加三块磁盘，选中已选磁盘可以在【选择空间量】文本框中输入创建的新分区从该磁盘调用的空间大小，所选的多块磁盘会调用相同大小的空间。配置完成后单击【下一步】按钮，如图 12-37 所示。

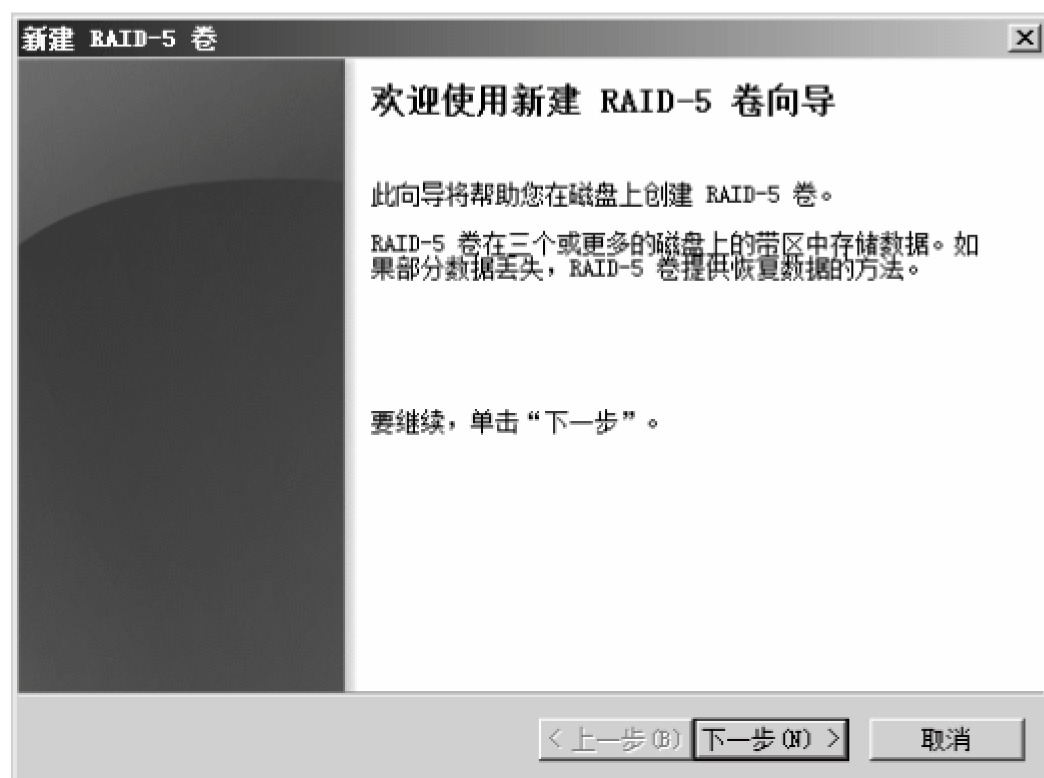


图 12-36　【新建 RAID-5 卷】对话框

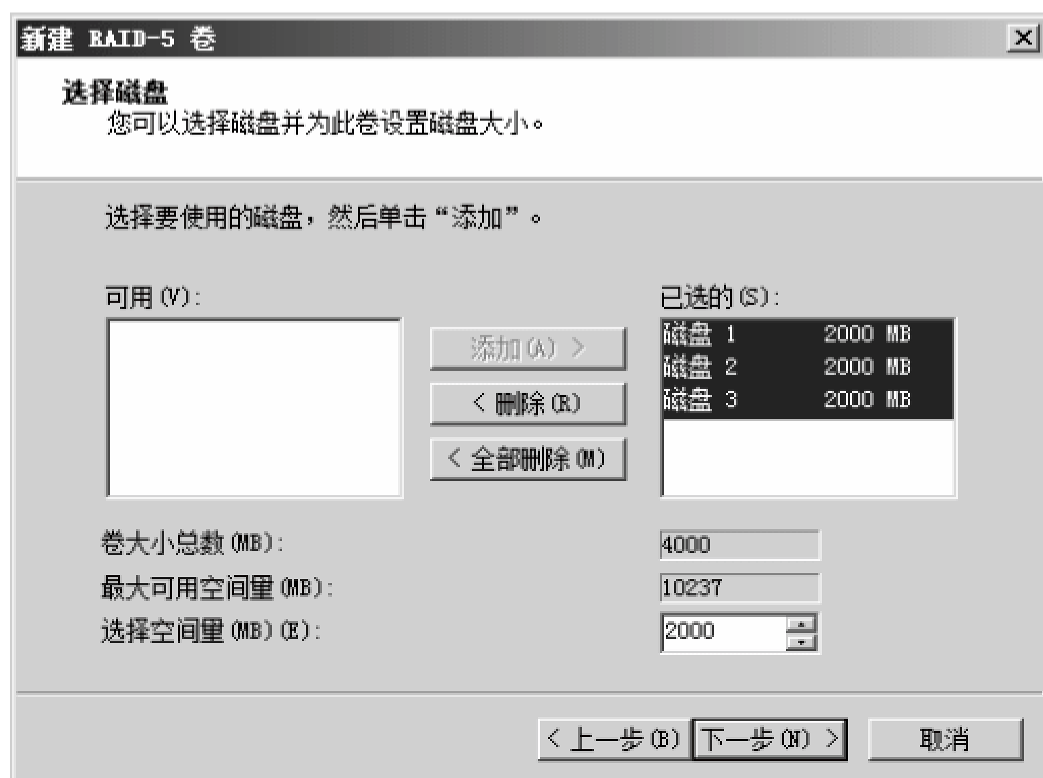


图 12-37　【选择磁盘】对话框

04 弹出【分配驱动器号和路径】对话框，选中【分配以下驱动器号】单选按钮，在后面的下拉列表框中选择合适的盘符号，单击【下一步】按钮，如图 12-38 所示。

05 弹出【卷区格式化】对话框，选中【按下列设置格式化这个卷】单选按钮，其他采用默认配置，单击【下一步】按钮，如图 12-39 所示。

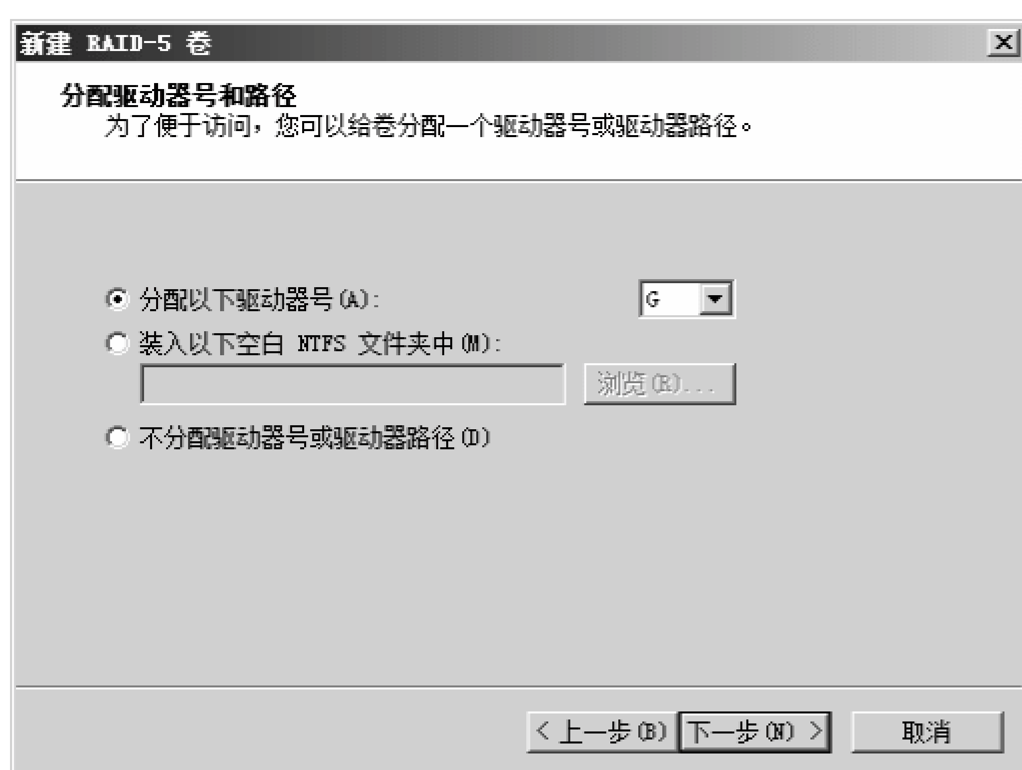


图 12-38　【分配驱动器号和路径】对话框

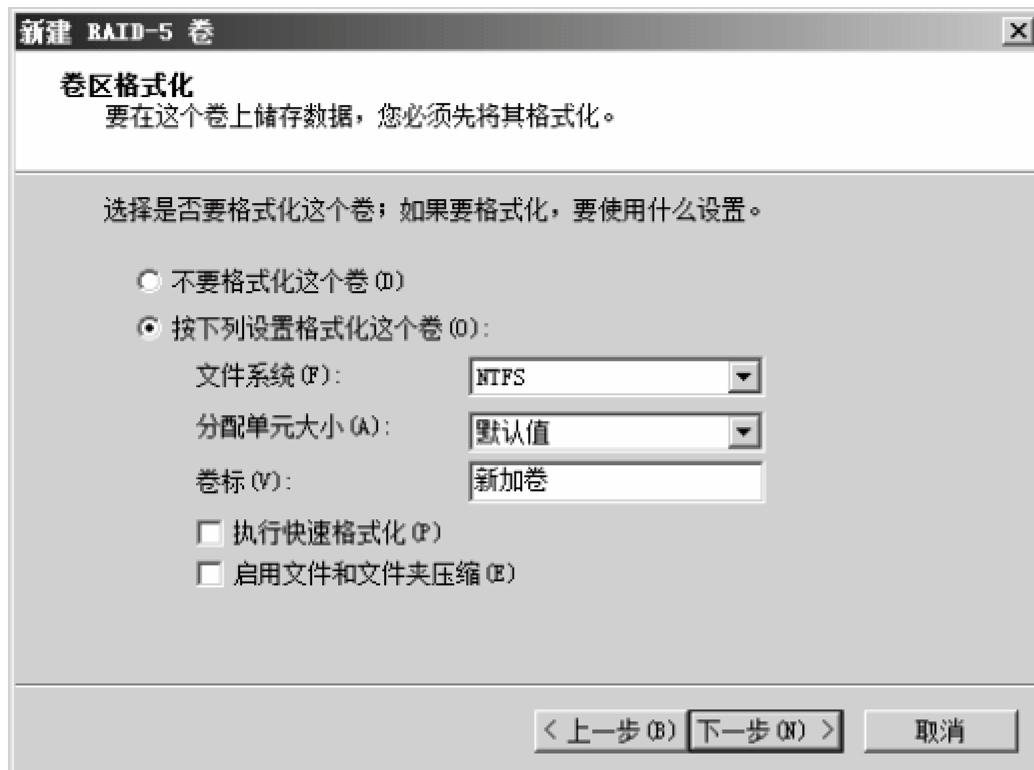


图 12-39　【卷区格式化】对话框

06 弹出【正在完成新建 RAID-5 卷向导】对话框，显示配置信息，单击【完成】按钮，如图 12-40 所示。

07 返回磁盘管理列表，新的 RAID-5 卷已经创建成功，并显示为蓝色，如图 12-41 所示。

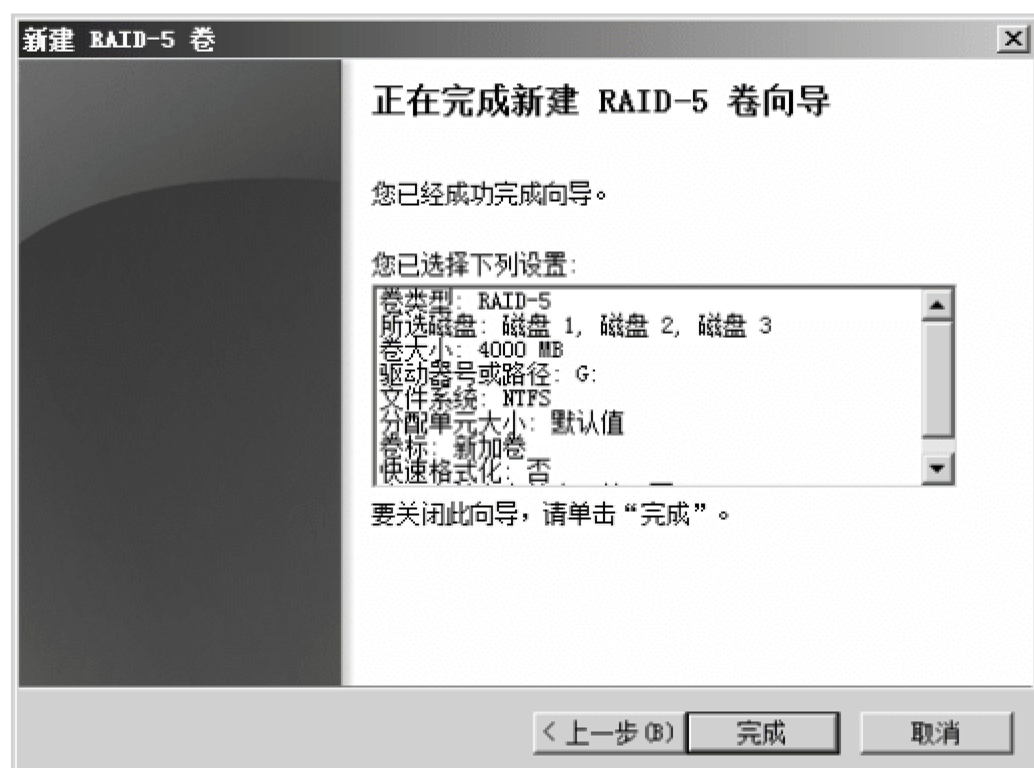


图 12-40 【正在完成新建 RAID-5 卷向导】对话框

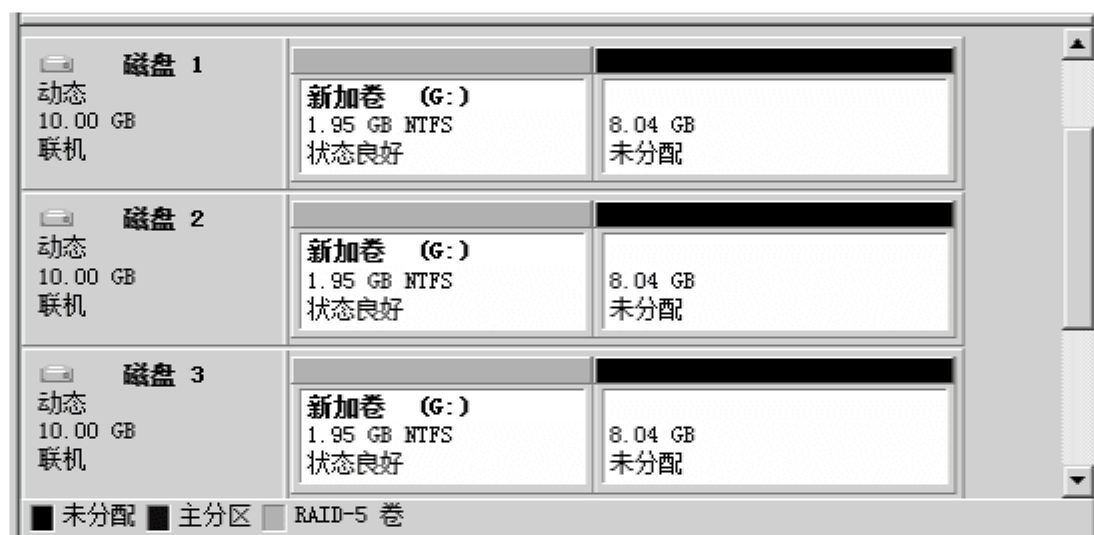


图 12-41 RAID-5 卷创建成功

12.2.2 为账户设定磁盘配额

作为存储服务器，可能会同时为多个远程用户提供存储空间，如 FTP、E-Mail 服务器连接的存储服务器就需要为多个 FTP 账户或邮箱账户提供空间。存储服务器的磁盘空间也是有限的，不可能无限制地为用户提供可用空间，当一个用户使用过多空间时，其他用户就没有充足空间可用了。所以在 Windows Server 系统中内置了账户磁盘配额限制功能。

Windows Server 中的磁盘配额功能主要对磁盘分区进行配置的，可以限制每一个账户使用指定磁盘分区的空间大小。为账户设定磁盘配额的具体操作步骤如下。

01 打开 Windows 资源管理器窗口，右击要创建磁盘配额的分区，在弹出的快捷菜单中选择【属性】命令，如图 12-42 所示。

02 弹出【本地磁盘（G:）属性】对话框，选择【配额】选项卡，如图 12-43 所示。选中【启用配额管理】复选框，启用该分区的配额功能。选中【拒绝将磁盘空间给超过配额限制的用户】复选框，确保磁盘配额限制生效。在【为该卷上的新用户选择默认配额限制】选项域，选中【将磁盘空间限制为】单选按钮，并设置后续新建账户使用此分区的空间限制，【将警告等级设为】文本框的值表示账户使用空间到达 90MB 时发出空间不足警告。单击【配额项】按钮，进行更多配额配置。

03 弹出【（G:）的配额项】窗口，可以对 G 盘做更多的磁盘配额设置。默认显示该分区对管理员账户组的配额限制，如图 12-44 所示。

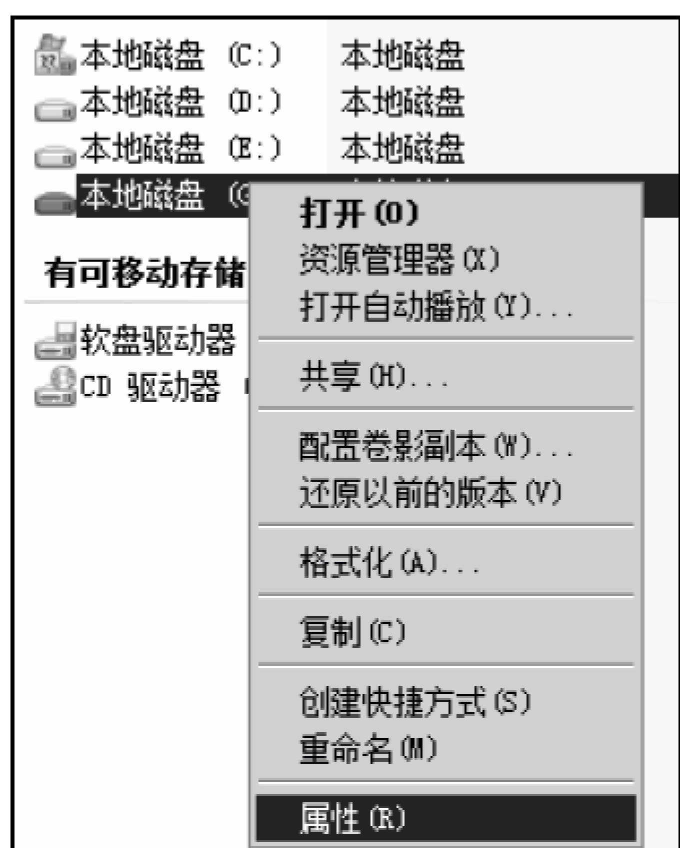


图 12-42　本地磁盘菜单选项

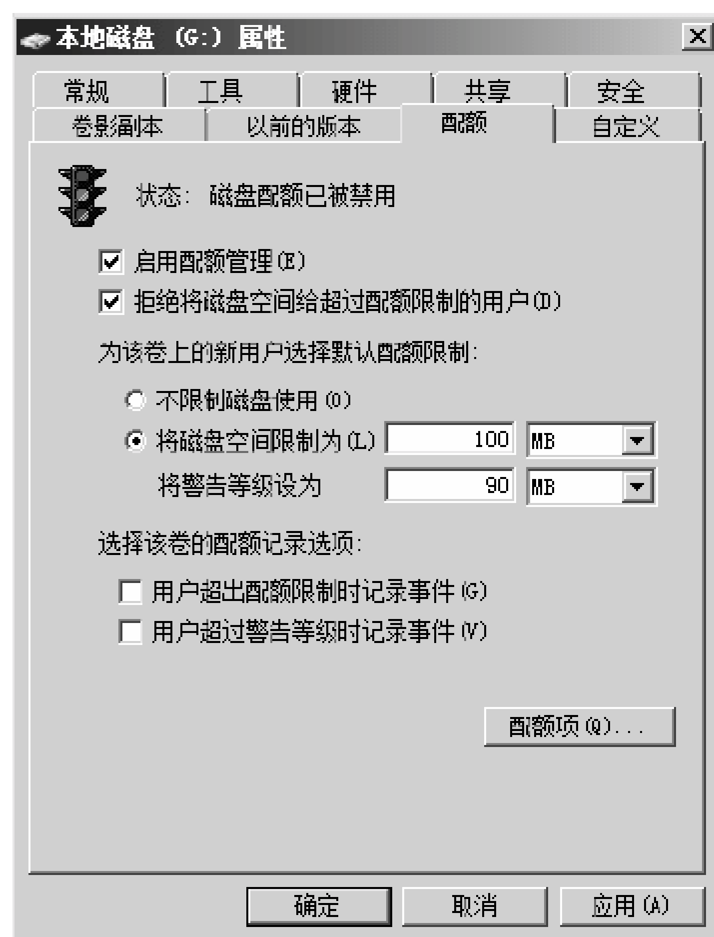


图 12-43　【本地磁盘（G:）属性】对话框



图 12-44　【（G:）的配额项】窗口

04 在菜单栏选择【配额】➢【新建配额项】命令，如图 12-45 所示。

05 弹出【选择用户】对话框，在文本框中输入要创建配额的账户，或者通过【高级】按钮添加账户，然后单击【确定】按钮，如图 12-46 所示。

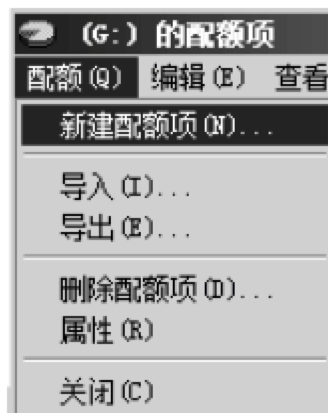


图 12-45　【配额】菜单选项



图 12-46　【选择用户】对话框

06 弹出【添加新配额项】对话框，设置配额限制值，如图 12-47 所示。

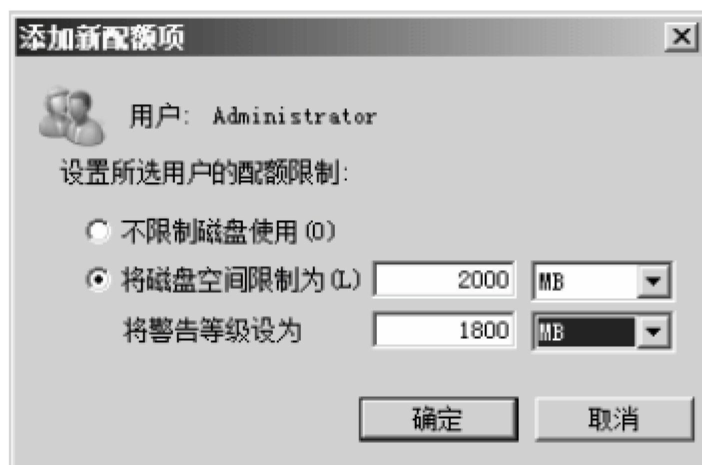


图 12-47　【添加新配额项】对话框

07 返回【（G:）的配额项】窗口，新添加的配额显示状态为正常，如图 12-48 所示。

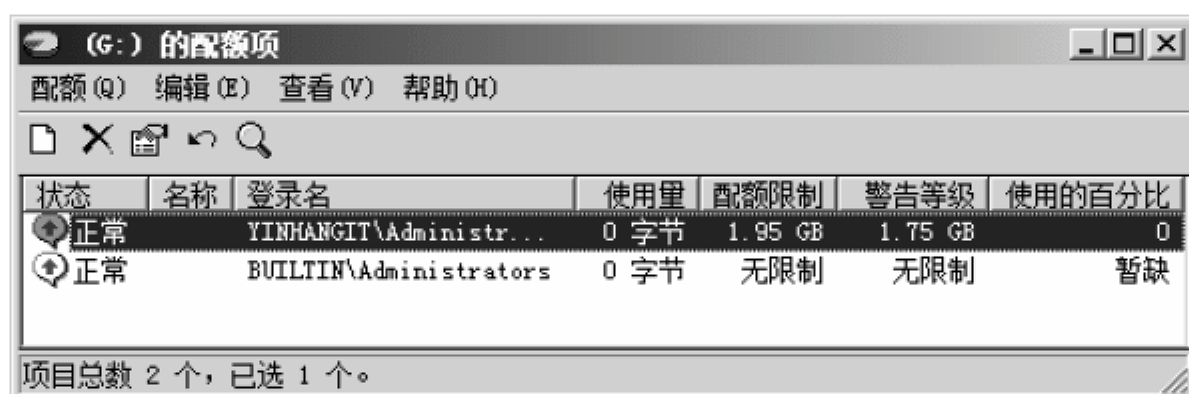


图 12-48　新账户配额添加成功

12.2.3　设定系统的数据备份计划

系统数据存放在存储服务器上，难免会发生意外致使存储服务器损坏。一旦损坏所有的数据都有可能会丢失，这就需要做好及时的备份，方便故障时做数据恢复。

存储服务器上的数据时时刻刻都在更新，作为管理者不可能每天都抽出时间去进行数据备份，这就需要系统能够自动按照一定的计划完成备份任务，Windows Server 中提供了数据备份功能。一般备份的时候必须要准备独立的空磁盘进行数据备份，且空间要充足，具体的操作方法如下。

1. 添加 Windows Server Backup 功能

Windows Server Backup 功能是 Windows Server 2008 中内置的数据备份功能，默认没有安装，安装该备份功能的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，选择左侧【功能】选项，如图 12-49 所示，在右侧单击【添加功能】选项。



图 12-49　【服务器管理器】窗口

02 弹出【添加功能向导】对话框，在【功能】选项列表中选中 Windows Server Backup 功能选项，该选项有两个子选项，如果管理员习惯使用命令行操作，可以考虑安装【命令行工具】选项，如图 12-50 所示，单击【下一步】按钮。

03 弹出【确认安装选择】对话框，如图 12-51 所示，单击【安装】按钮。

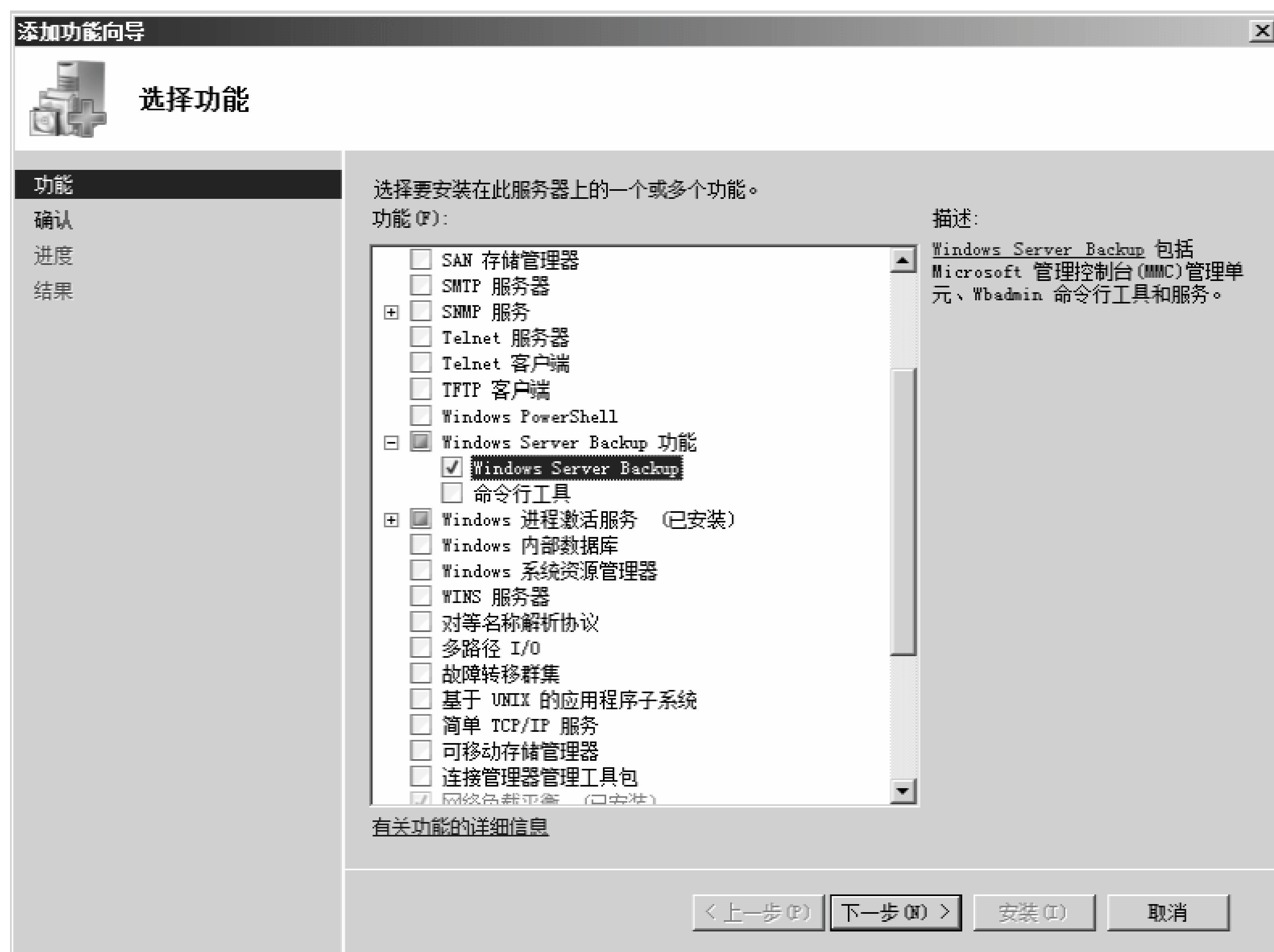


图 12-50 【添加功能向导】对话框



图 12-51 【确认安装选择】对话框

04 弹出【安装进度】对话框，系统自动安装 Windows Server Backup 组件，如图 12-52 所示。

05 安装完成后弹出【安装结果】对话框，单击【关闭】按钮结束安装向导，如图 12-53 所示。



图 12-52 【安装进度】对话框



图 12-53 【安装结果】对话框

2. 制定备份计划

安装完成之后可以制定备份计划，具体操作步骤如下。

01 选择【开始】➢【程序】➢【管理工具】➢ Windows Server Backup 命令，如图 12-54 所示。

02 弹出 Windows Server Backup 窗口，左侧窗格用于统计显示当前的备份配置及执行状态信息，选择右侧【操作】选项列表中的【备份计划】选项，如图 12-55 所示。

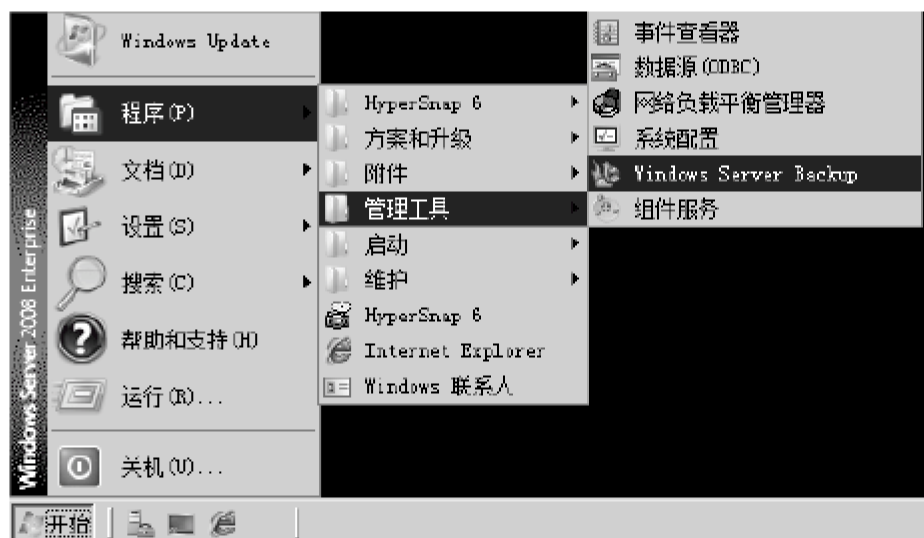


图 12-54　开始菜单选项

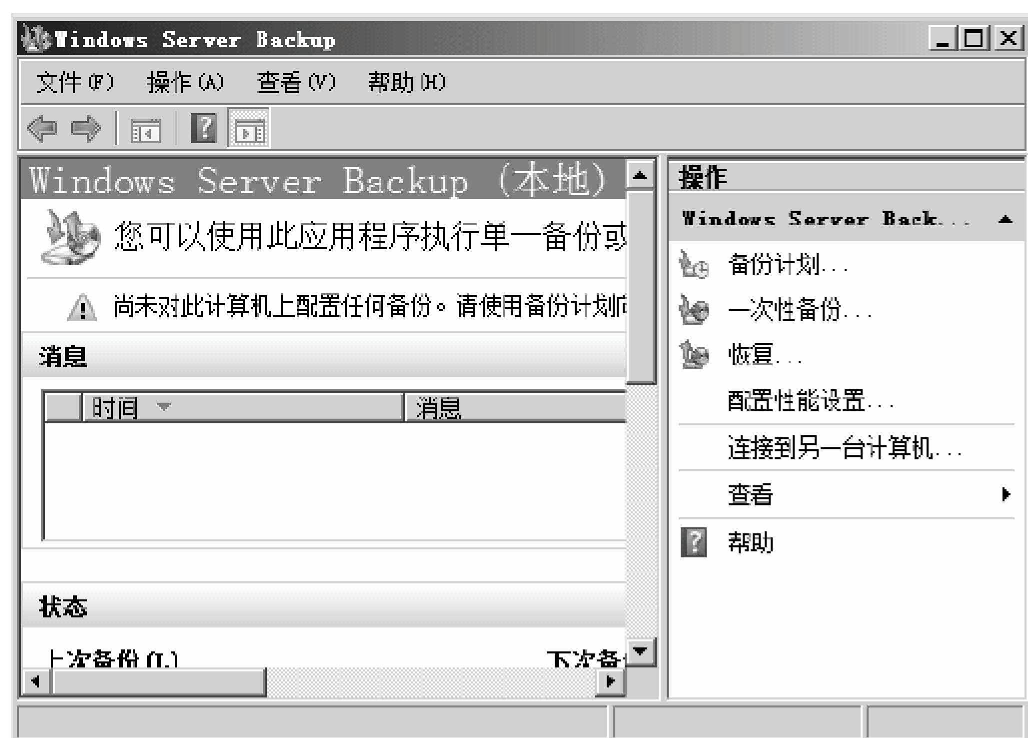
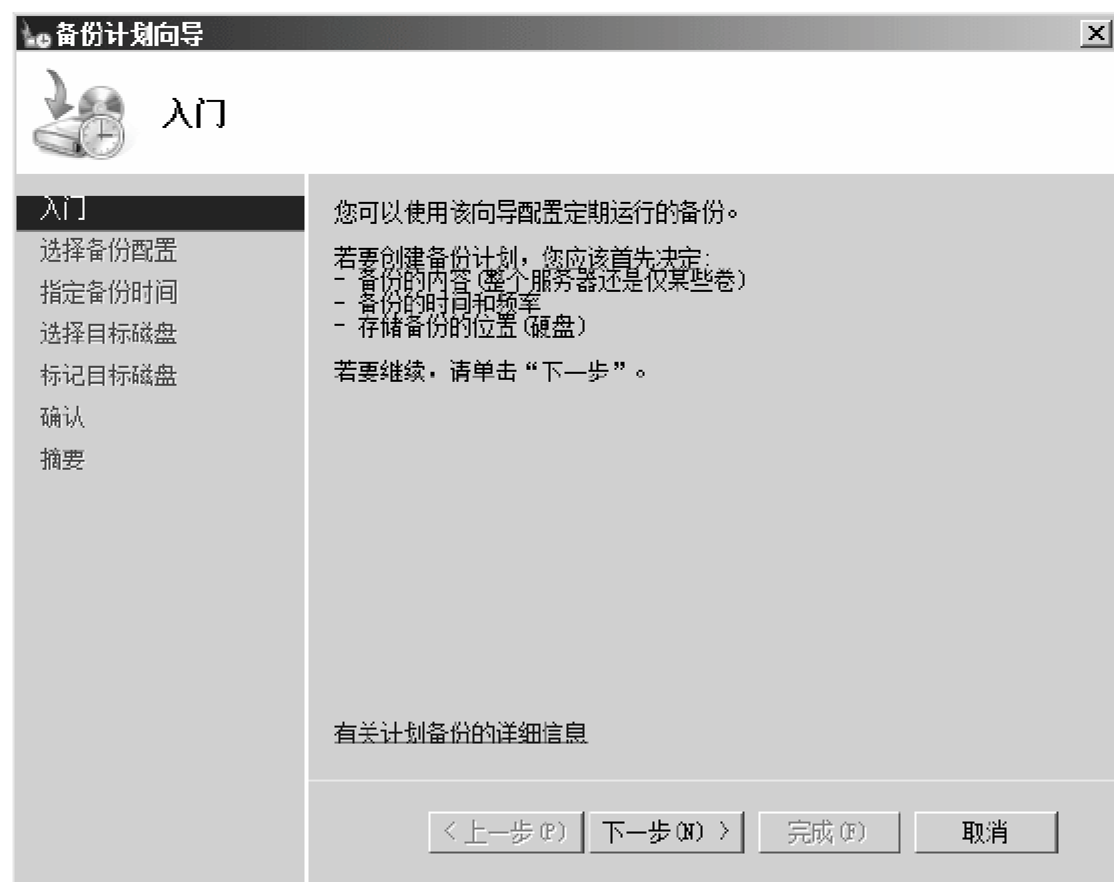


图 12-55　Windows Server Backup 窗口

03 弹出【备份计划向导】对话框，显示备份计划入门介绍信息，单击【下一步】按钮，如图 12-56 所示。

04 打开【选择备份配置】对话框，默认选中【整个服务器】单选按钮，可以将整个服务器的所有配置进行保存，也可以选中【自定义】单选按钮手工指定备份内容，本实例采用【自定义】，如图 12-57 所示。



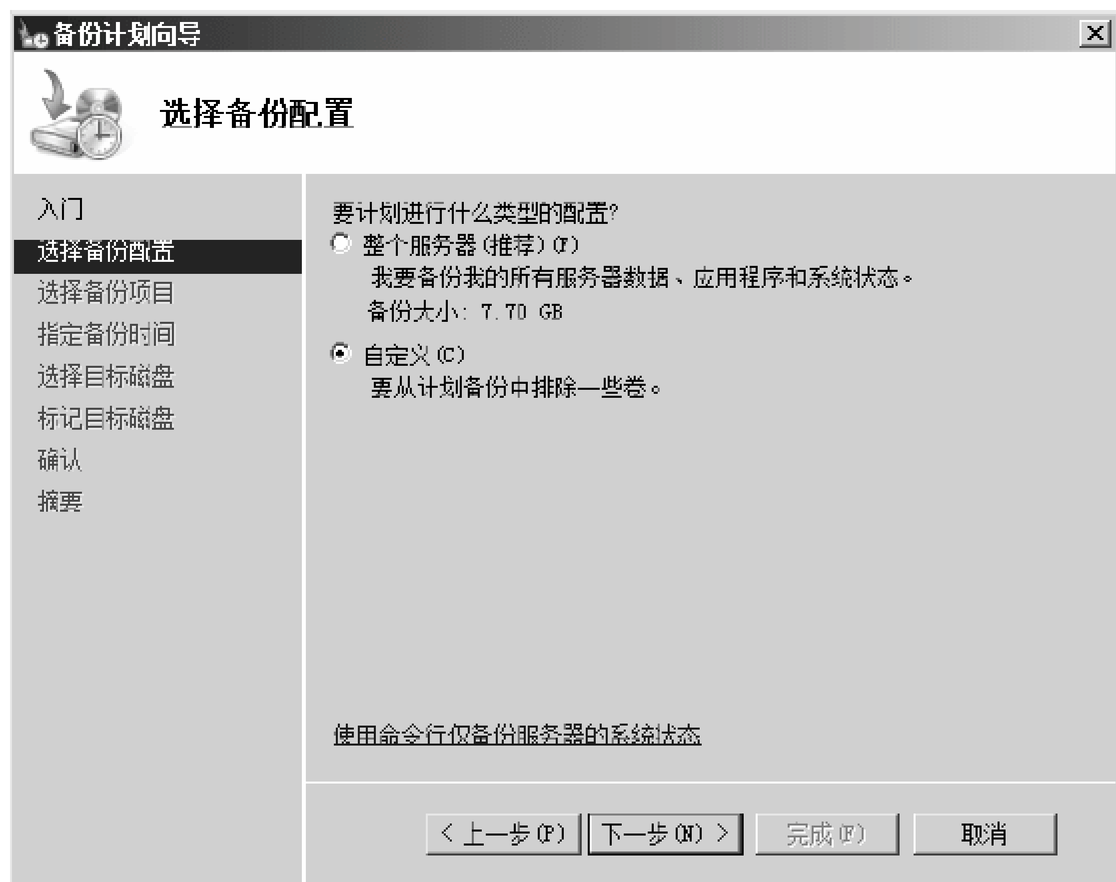


图 12-56　【备份计划向导】对话框　　　　图 12-57　【选择备份配置】对话框

05 打开【选择备份项目】对话框，在备份选项列表中显示了可以备份的卷，选择需要备份的卷，单击【下一步】按钮，如图 12-58 所示。

06 打开【指定备份时间】对话框，可以选中【每日一次】单选按钮，并在【选择时间】下拉列表框中选择时间，也可以选中【每日多次】单选按钮，并将需要进行备份的时间从左侧【可用时间】列表添加到右侧【已计划的时间】列表中，单击【下一步】按钮，如图 12-59 所示。

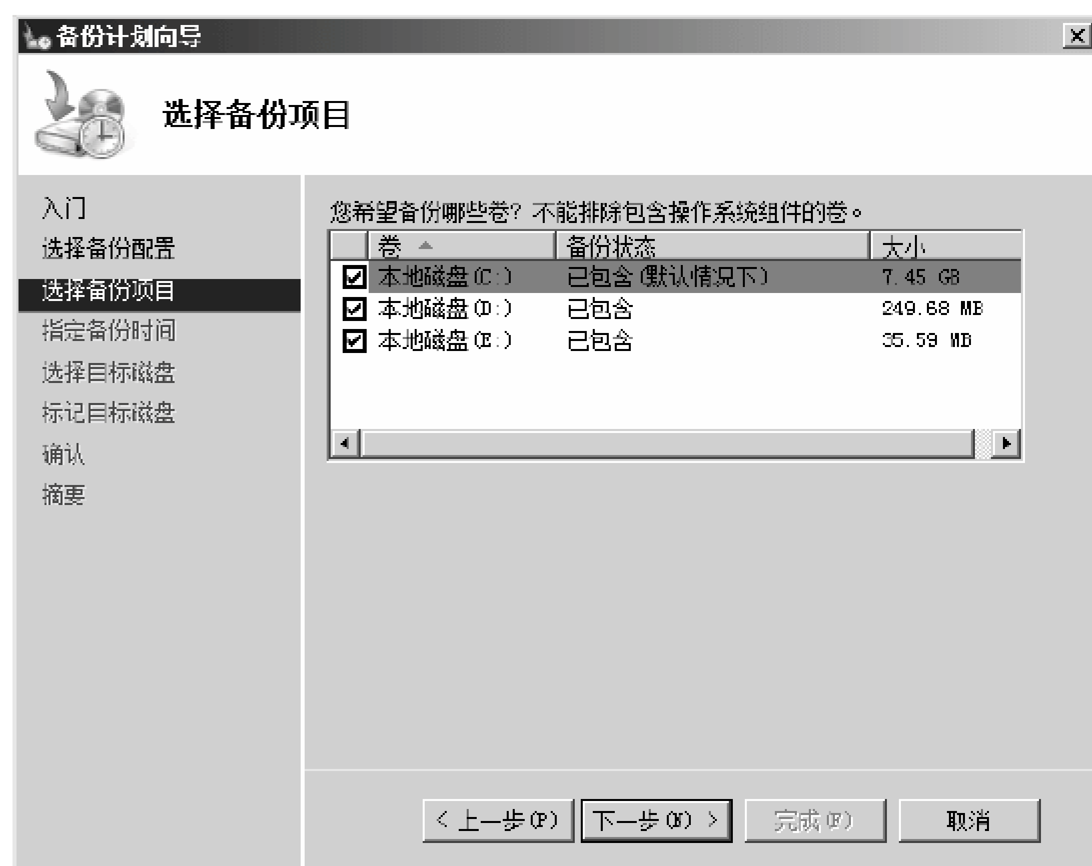


图 12-58 【选择备份项目】对话框

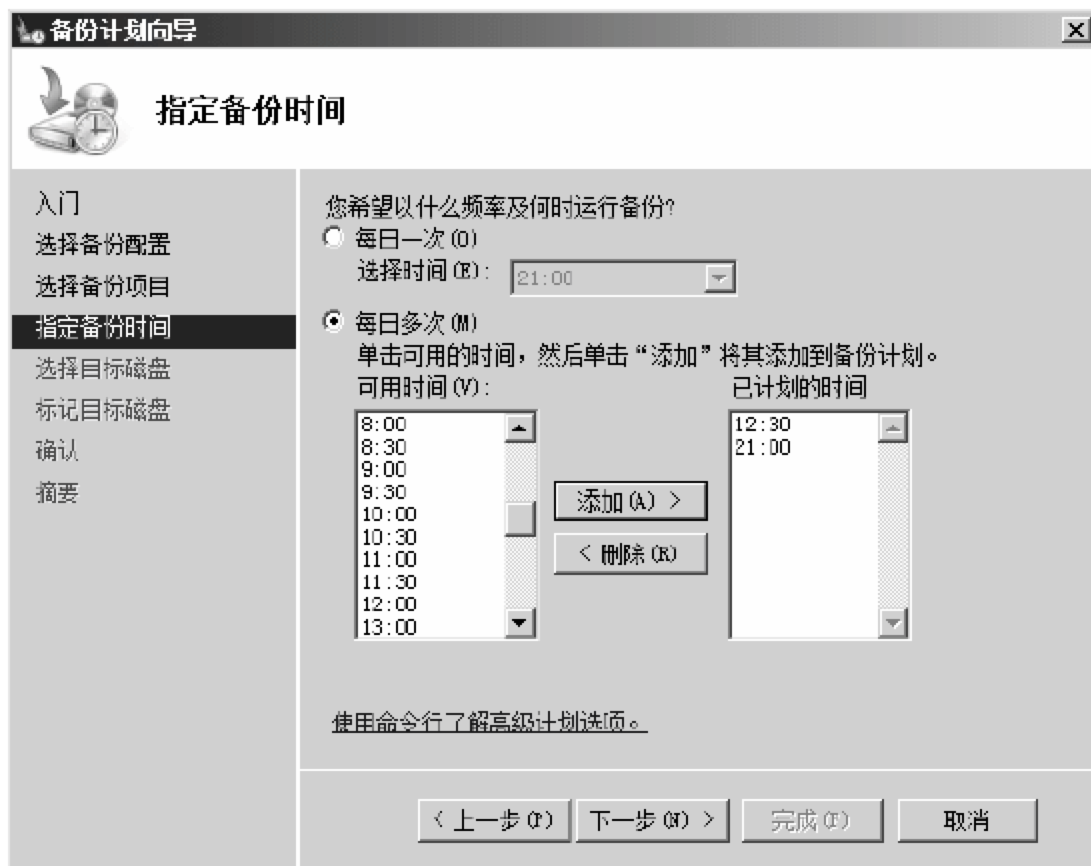


图 12-59 【指定备份时间】对话框

07 弹出【选择目标磁盘】对话框，单击【显示所有可用磁盘】按钮，如图 12-60 所示。

08 弹出【显示所有可用磁盘】对话框，在【所有磁盘】列表中选择要进行数据备份的磁盘（本实例是采用 VMware 创建的虚拟磁盘），单击【确定】按钮，如图 12-61 所示。

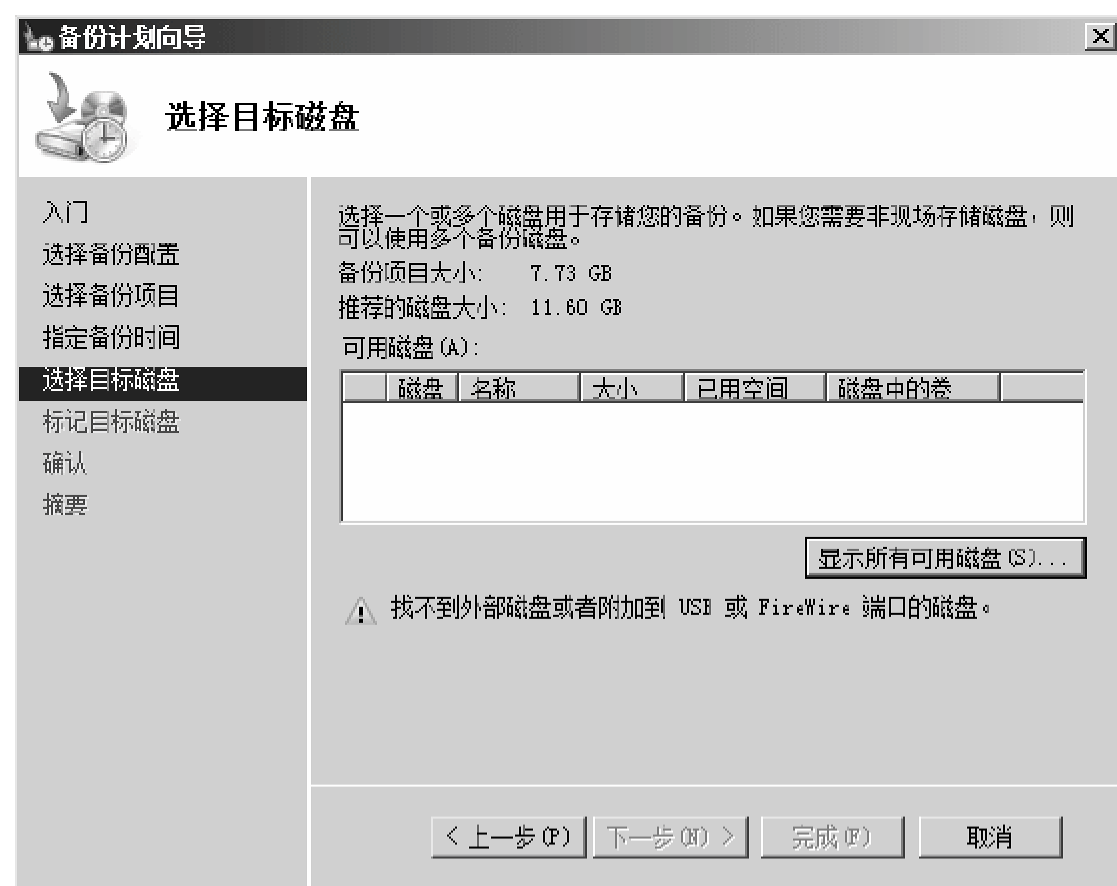


图 12-60 【选择目标磁盘】对话框

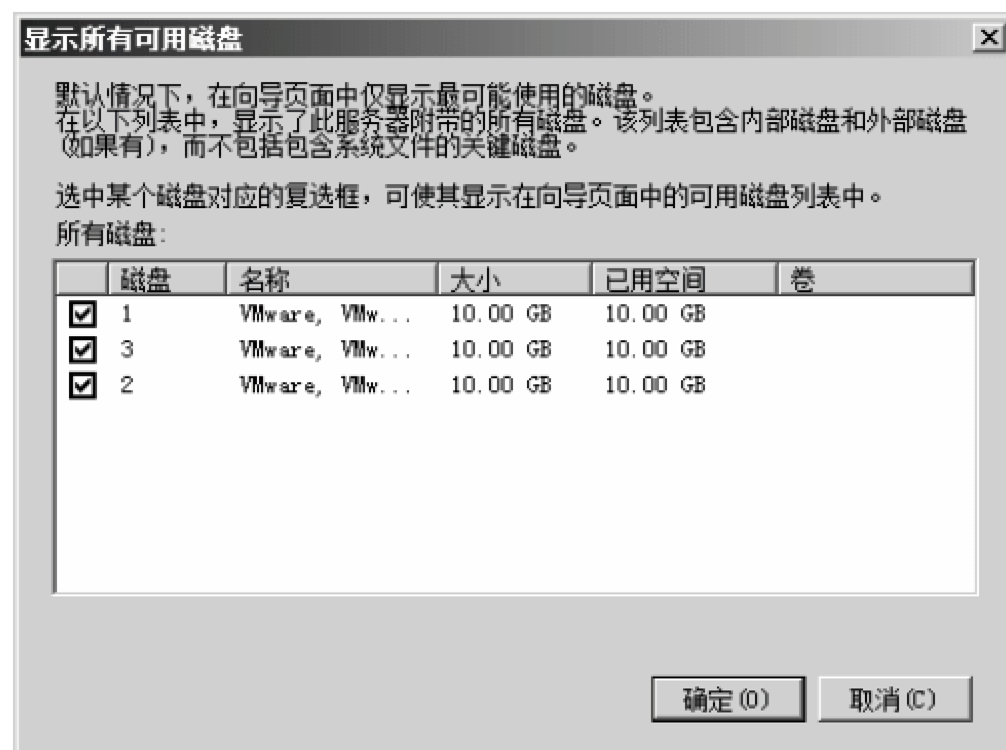


图 12-61 【显示所有可用磁盘】对话框

09 弹出【选择目标磁盘】对话框，备份的目标磁盘选择成功，单击【下一步】按钮，如图 12-62 所示。

10 弹出提示框，提示目标磁盘将被格式化，且要实现备份完整性，必须将目标磁盘专用于存储备份，单击【是】按钮，如图 12-63 所示。

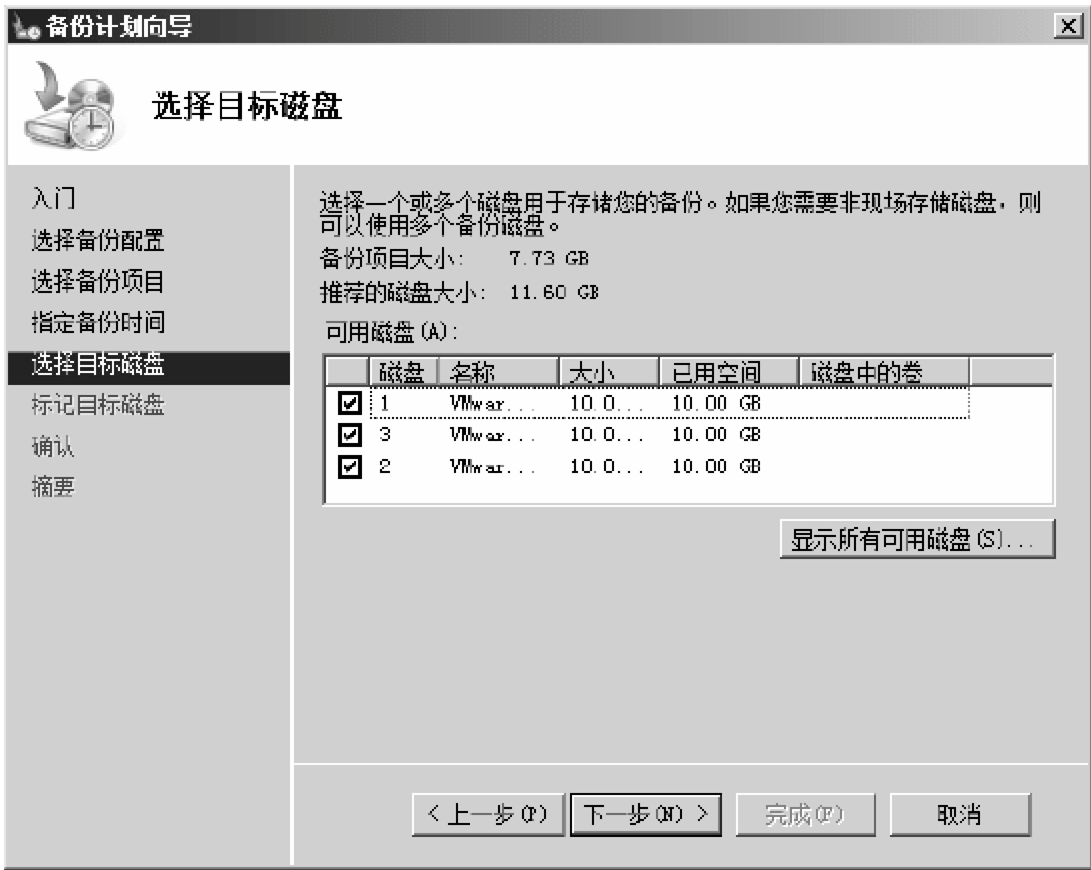


图 12-62　【选择目标磁盘】对话框



图 12-63　格式化提示框

11 弹出提示框，提示目标备份空间小于当前备份数据的 1.5 倍，空间过小可能导致以后追加备份内容失败，单击【确定】按钮，如图 12-64 所示。

12 弹出【标记目标磁盘】对话框，为目标磁盘增加标签，单击【下一步】按钮，如图 12-65 所示。

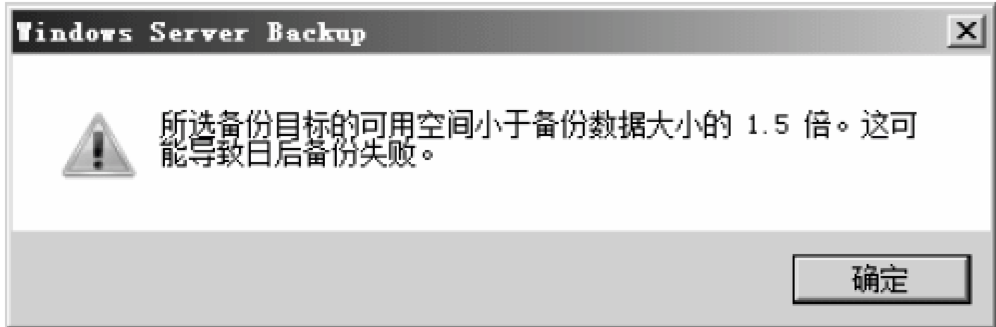


图 12-64　提示目标空间不充足

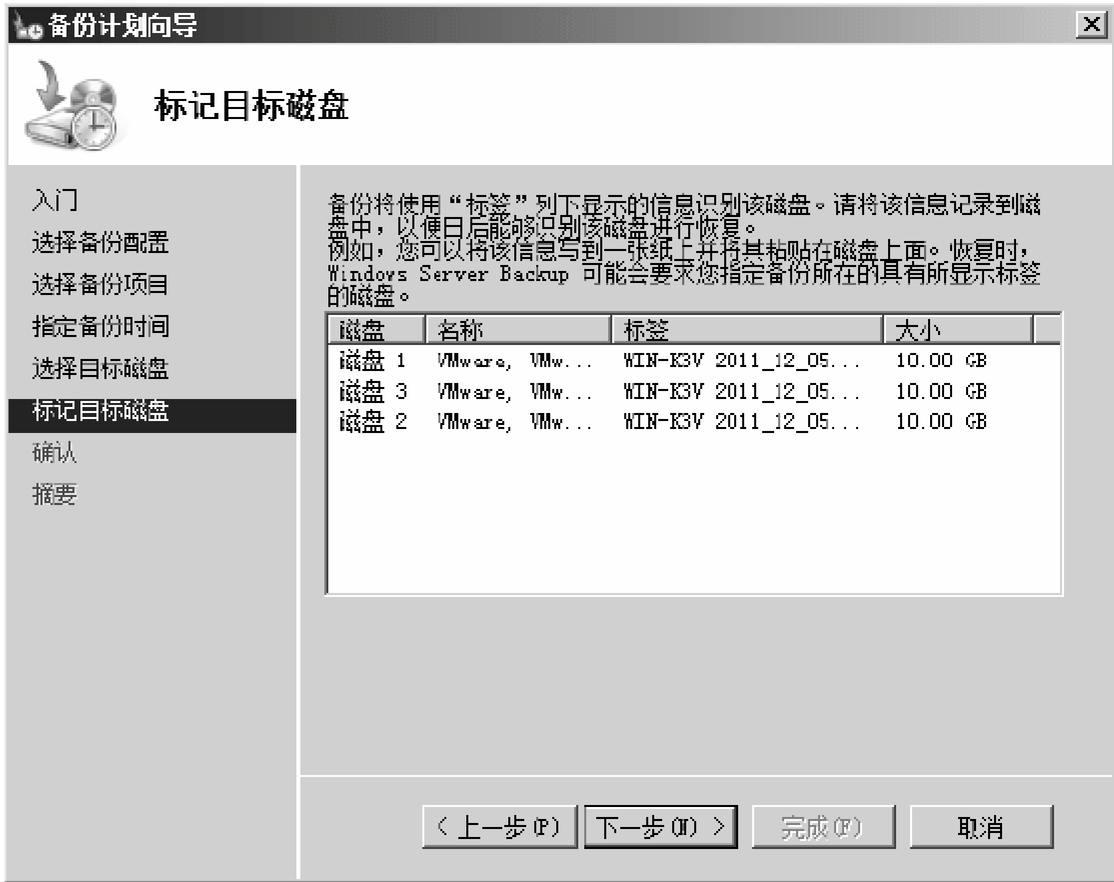


图 12-65　【标记目标磁盘】对话框

13 弹出【确认】对话框，显示备份配置信息，单击【完成】按钮，如图 12-66 所示。

14 弹出【摘要】对话框，格式化目标磁盘，并显示备份计划设置完成信息，如图 12-67 所示。

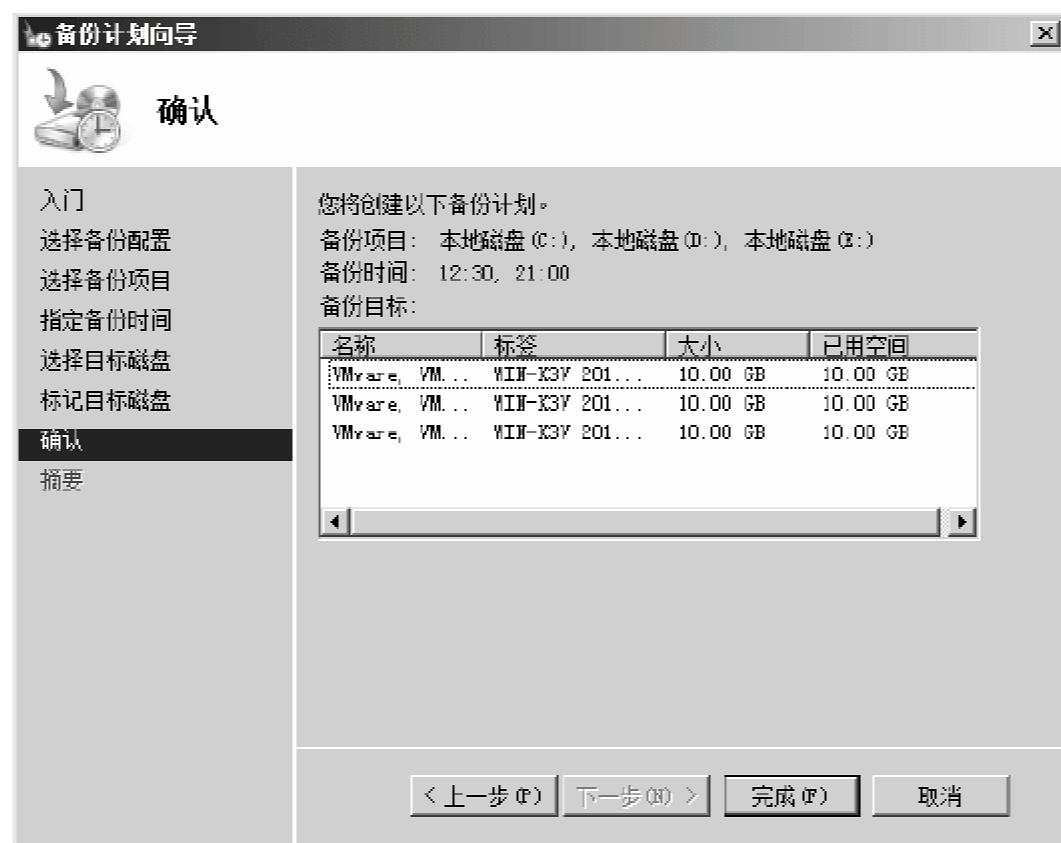


图 12-66 【确认】对话框

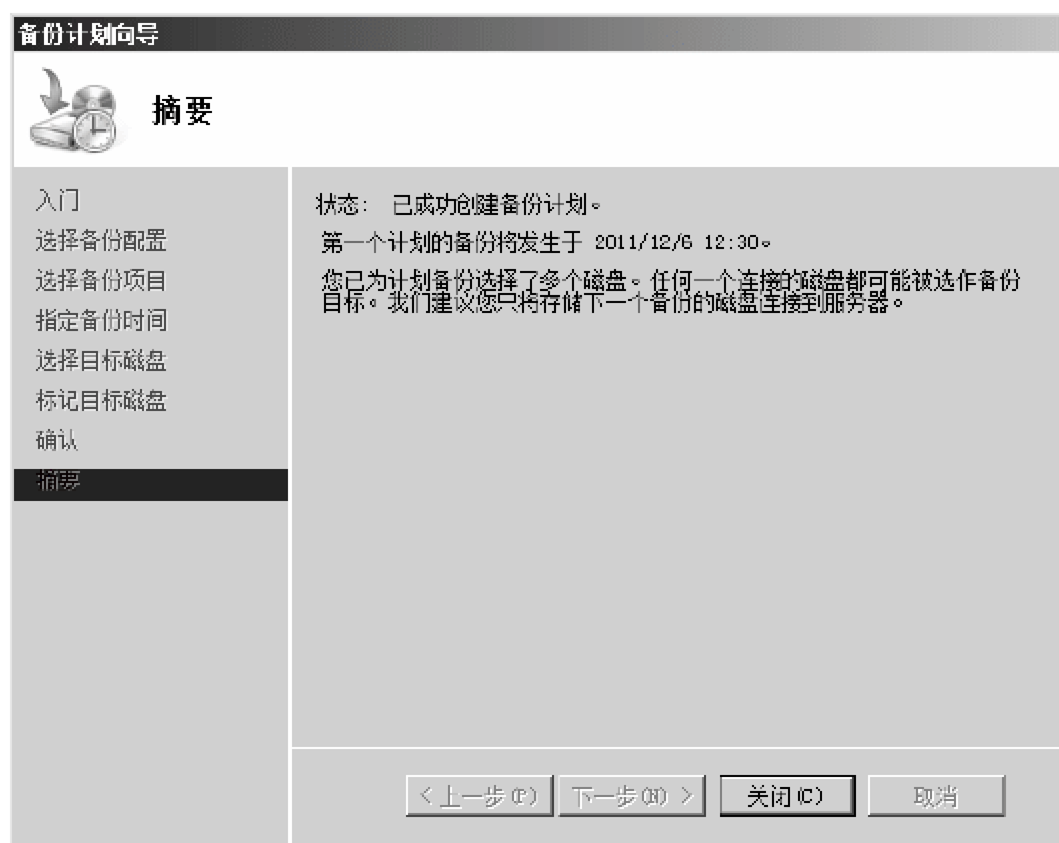


图 12-67 【摘要】对话框

3. 一次性备份数据

在特殊的情况下管理员可能需要临时备份数据，如要大规模停电、有地震洪涝灾害发生等。这时候备份计划可能还没有到时间，为了确保数据是完整的，管理员手动备份数据。

管理员手动一次性备份数据的具体操作步骤如下。

01 打开 Windows Server Backup 窗口，在右侧【操作】选项列表中选择【一次性备份】选项，如图 12-68 所示。

02 弹出【备份选项】对话框，选中【备份计划向导中用于计划备份的相同选项】单选按钮可以直接调用备份计划中的设置进行备份数据，也可以选中【不同选项】单选按钮重新设定备份配置，本实例选择使用备份计划中的配置，单击【下一步】按钮，如图 12-69 所示。



图 12-68 Windows Server Backup 窗口

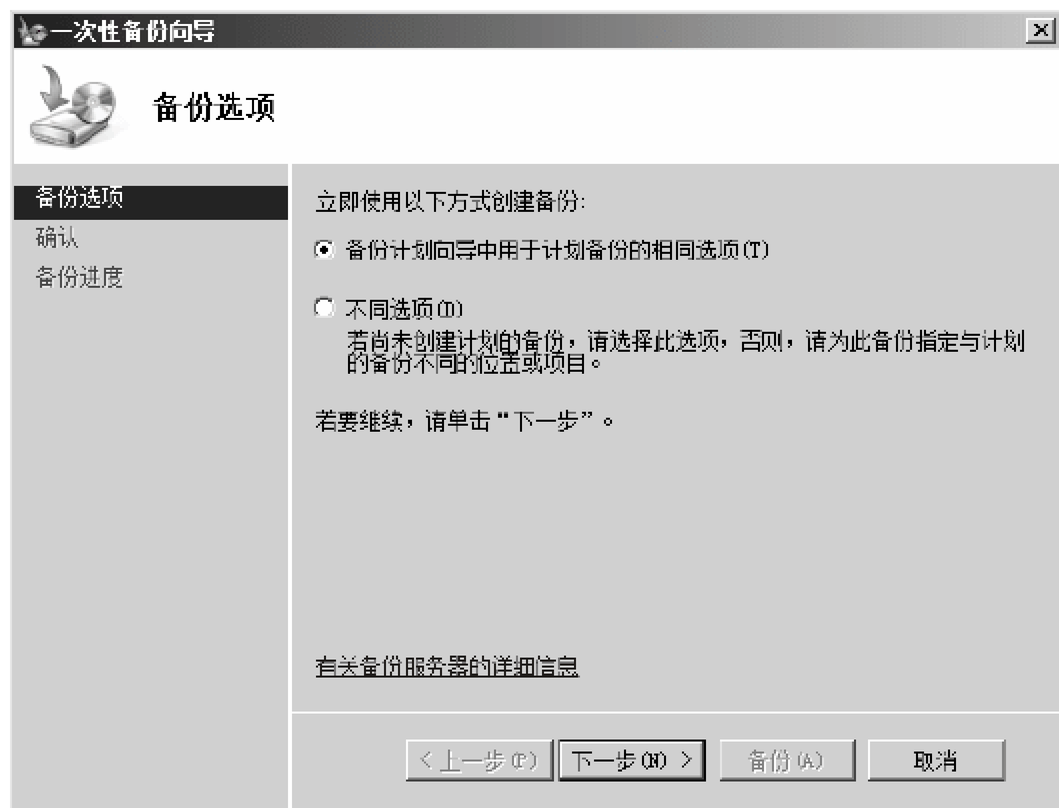


图 12-69 【备份选项】对话框

03 弹出【确认】对话框，显示备份计划中的配置，确认无误后单击【备份】按钮，如图 12-70 所示。

04 弹出【备份进度】对话框，逐一备份数据，并显示备份进度条，备份完成后单击【关闭】按钮，如图 12-71 所示。

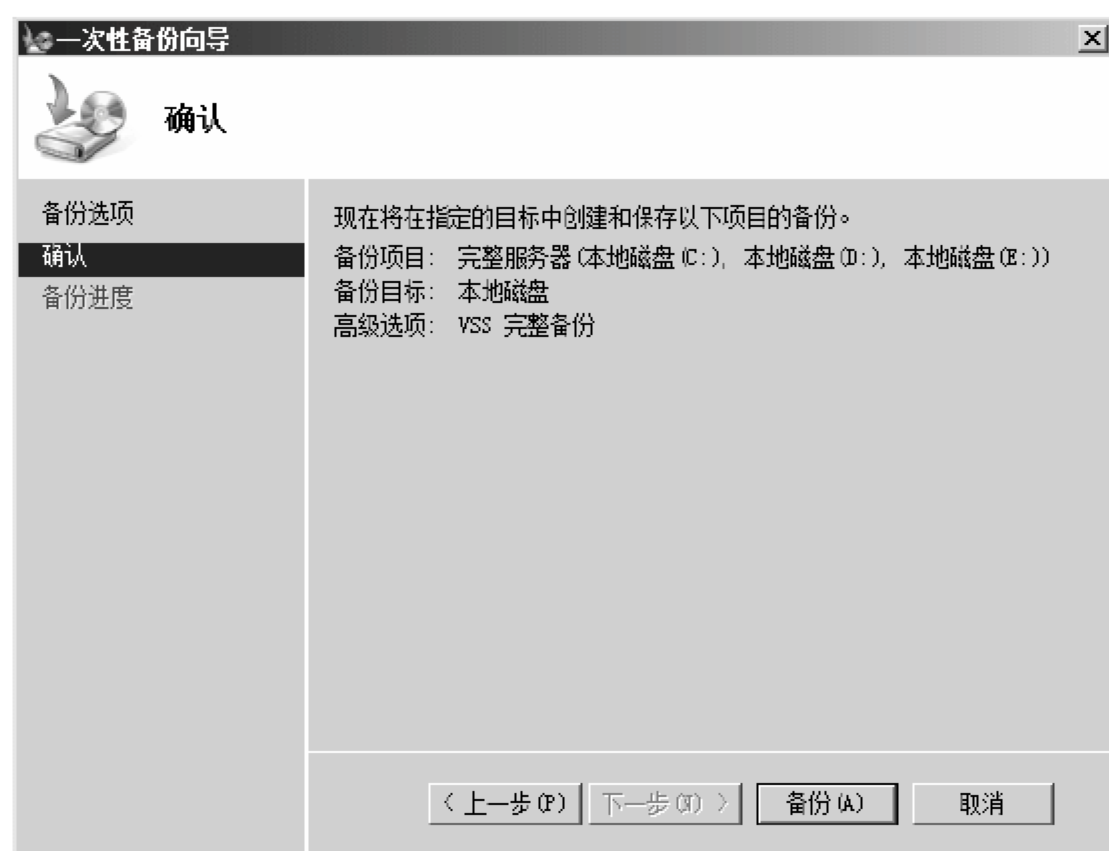


图 12-70　【确认】对话框



图 12-71　【备份进度】对话框

4. 恢复数据

备份的目的就是在数据或系统损坏时可以及时恢复。恢复备份数据的具体操作步骤如下。

01 打开 Windows Server Backup 窗口，在右侧【操作】选项列表中选择【恢复】选项，如图 12-72 所示。

02 弹出【入门】对话框，选择恢复数据源，选中【此服务器】单选按钮，表示要恢复的备份数据连接在本地服务器上，单击【下一步】按钮，如图 12-73 所示。

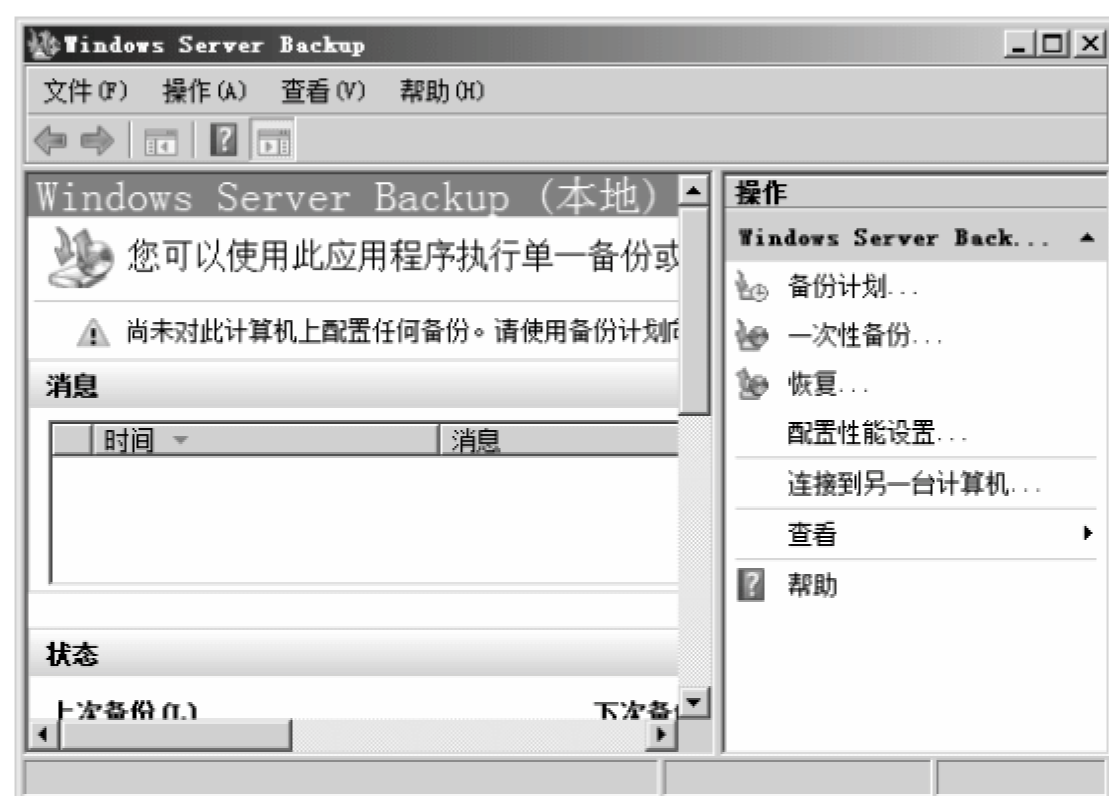


图 12-72　Windows Server Backup 窗口

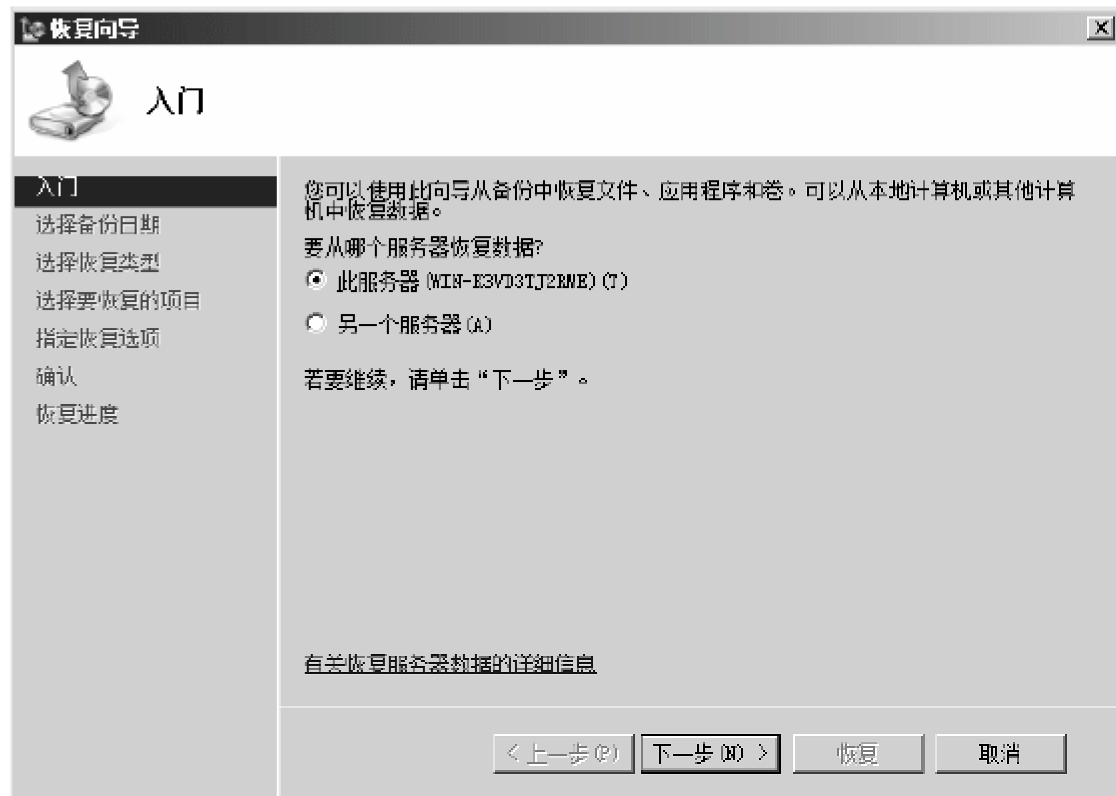


图 12-73　【入门】对话框

03 弹出【选择备份日期】对话框，选择要恢复的备份数据时间，本实例中只备份了一次，时间为 2011 年 12 月 5 日 22 时 44 分，单击【下一步】按钮，如图 12-74 所示。

04 弹出【选择恢复类型】对话框，选择要恢复数据的方式，可以指定文件或文件夹恢复，也可以指定整个卷进行恢复，本实例选中【文件和文件夹】单选按钮，单击【下一步】按钮，如图 12-75 所示。



图 12-74 【选择备份日期】对话框

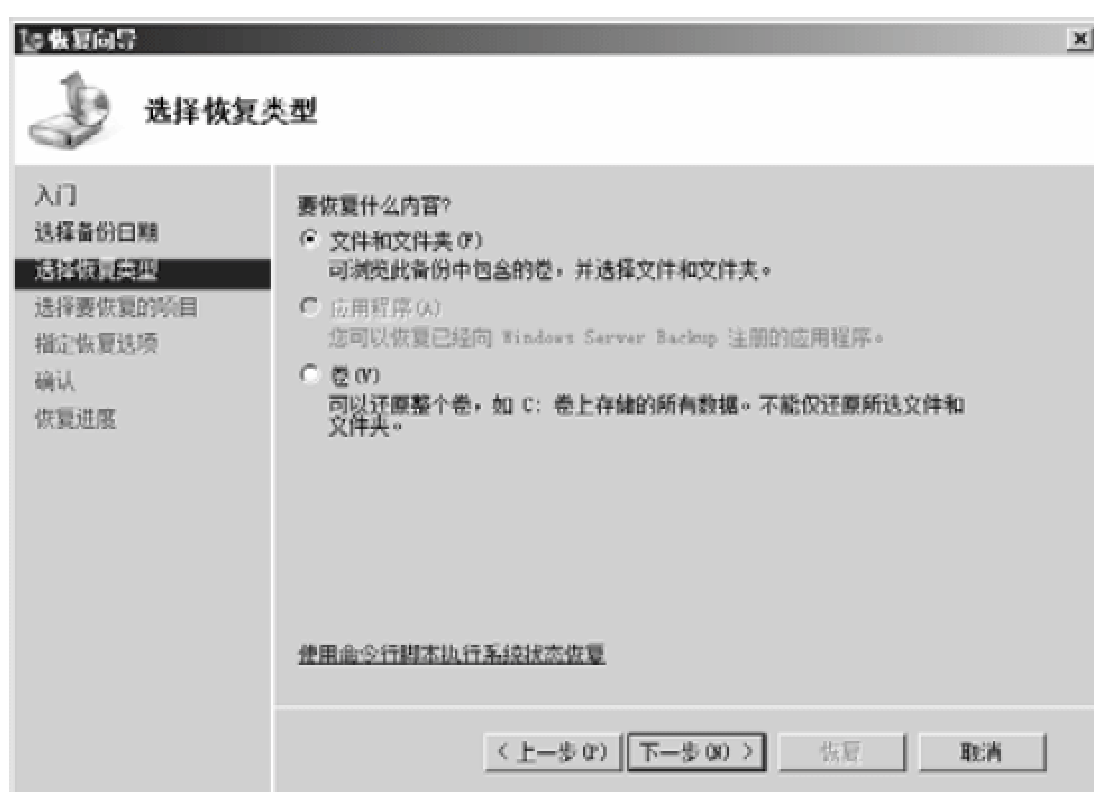


图 12-75 【选择恢复类型】对话框

05 弹出【选择要恢复的项目】对话框，在【可用项目】列表中选择要恢复的数据文件和文件夹，右侧列表中显示的是已经确认要恢复的数据，添加完成后单击【下一步】按钮，如图 12-76 所示。

06 弹出提示框，提示数据无法恢复到原始位置，当前系统正在运行恢复到原始位置要覆盖原来的数据，单击【确定】按钮，如图 12-77 所示。

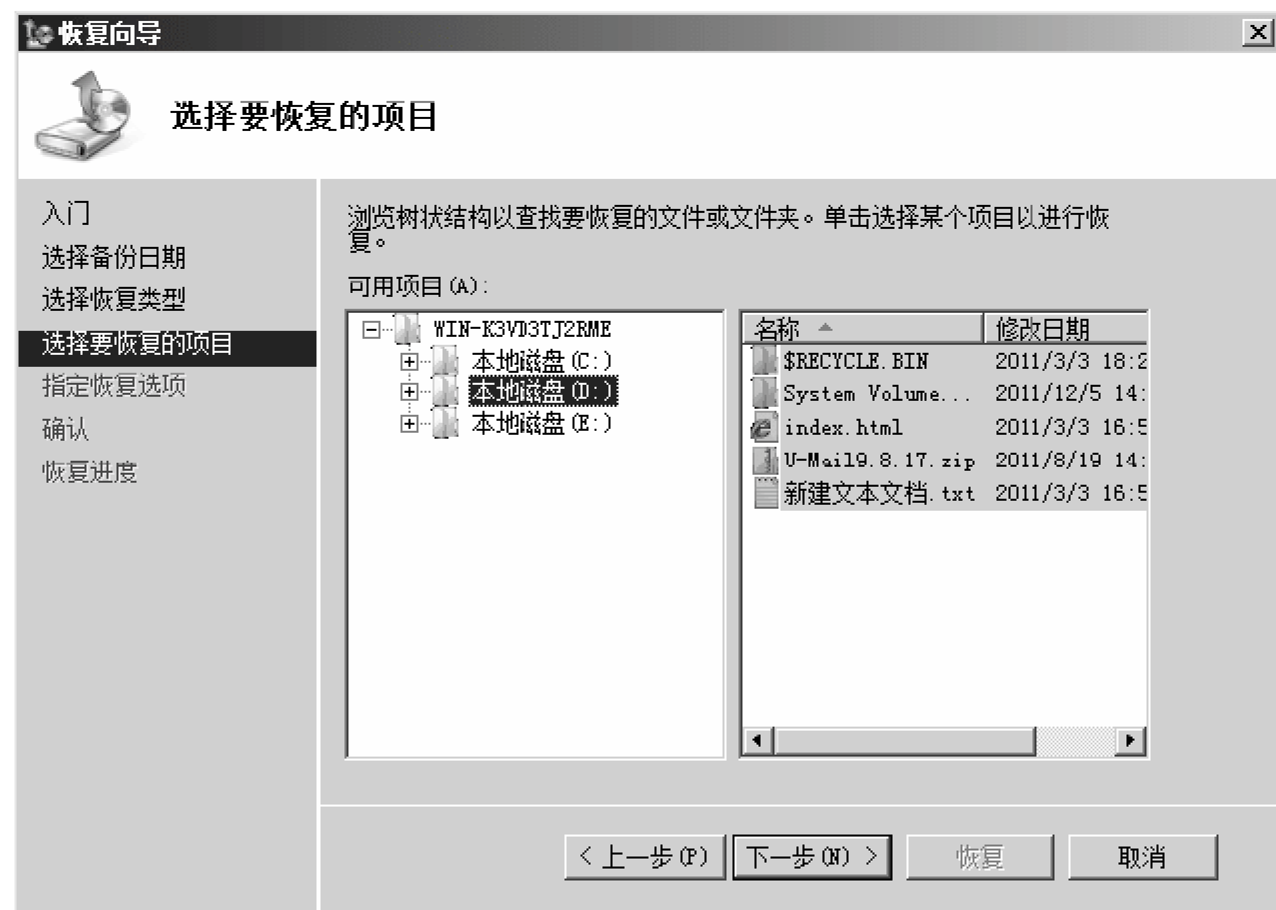


图 12-76 【选择要恢复的项目】对话框

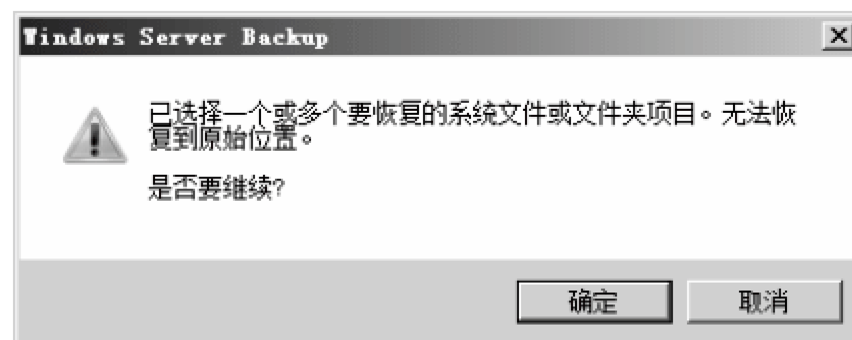


图 12-77 数据恢复提示框

07 弹出【指定恢复选项】对话框，指定数据恢复的目标位置和恢复选项，本实例将数据恢复到 E 盘，单击【下一步】按钮，如图 12-78 所示。

08 弹出【确认】对话框，显示恢复配置信息，确认后单击【恢复】按钮，如图 12-79 所示。



图 12-78　【指定恢复选项】对话框

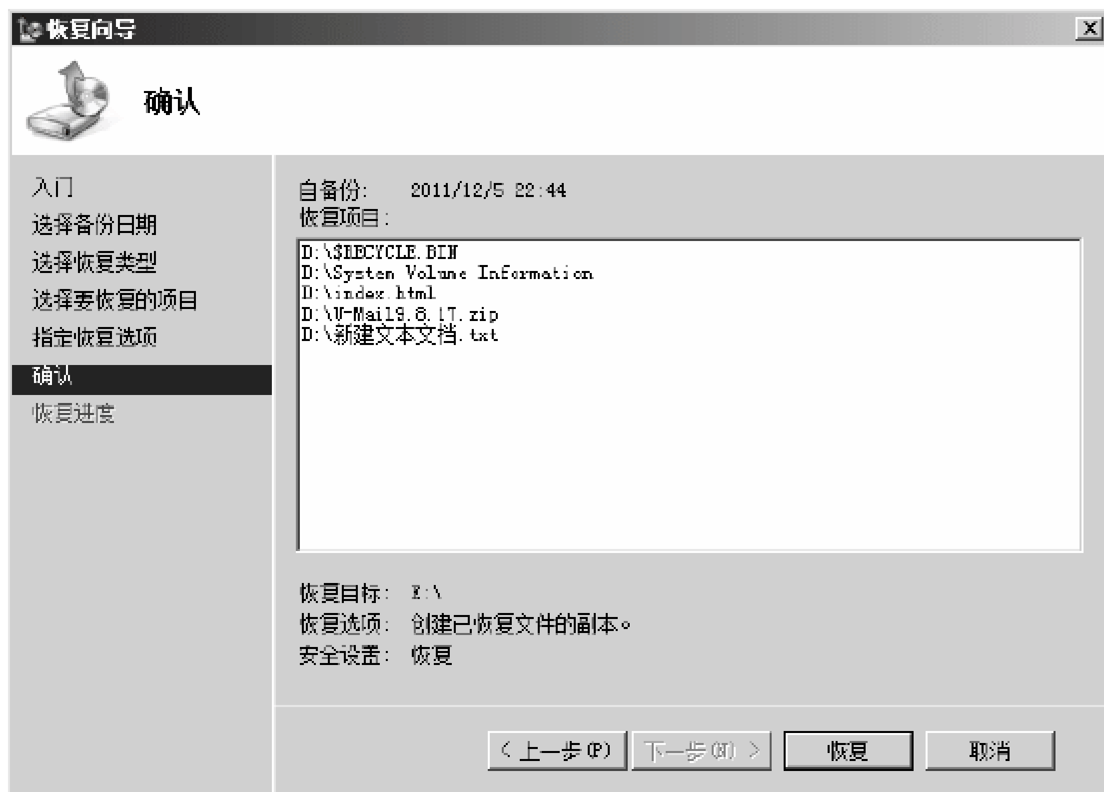


图 12-79　【确认】对话框

09　弹出【恢复进度】对话框，开始逐一恢复数据，如图 12-80 所示。

10　数据恢复完成，单击【关闭】按钮，如图 12-81 所示。



图 12-80　【恢复进度】对话框



图 12-81　数据恢复完成

12.3　项目实战 2：使用磁盘阵列柜

企业网络中用做存储的设备是磁盘，但是面对大量的企业存储信息，单靠普通的一两块磁盘根本不能满足需求，所以就产生了磁盘阵列柜。本节主要讲解磁盘阵列柜的概念，以及磁盘阵列中磁盘损坏后的恢复方法。

12.3.1　认识磁盘阵列柜

磁盘阵列柜是可以将多块磁盘整合为一个磁盘组，提供更大分区空间、更高的读写速度、更好的数据安全性保护。磁盘阵列柜中主要使用的就是磁盘阵列技术，而磁盘阵列技术可以将多块磁盘整合成为一个大的存储空间，并实现多块磁盘同时读写，构建冗余，以提升数据读写速度与安全性。

使用磁盘阵列技术可以将廉价、容量小、稳定性高、速度慢的多个磁盘组成一个大的磁盘组，这样可以使磁盘存储跟上性能不断提高的 CPU 和内存等设备，更好地发挥机器性能。

磁盘阵列柜可以同时连接至少 6 块的磁盘数量，大型的设备甚至可以同时连接 30 多块磁盘。图 12-82 所示是可以连接 12 块磁盘的磁盘阵列柜，可以通过磁盘阵列柜后面板的数据线连接到服务器上。



图 12-82　插 12 块磁盘的磁盘阵列柜

12.3.2　存储磁盘损坏后的数据恢复

当磁盘阵列柜中的某一块磁盘损坏后，可以通过其他磁盘的冗余数据进行数据恢复重建。创建的卷使用不同的磁盘阵列技术，恢复的方法也有所差异。下面介绍常用的镜像卷和 RAID-5 卷数据恢复的方法。

1. 镜像卷恢复重建

构成镜像卷的两块磁盘保存有相同的数据内容，当一块磁盘损坏后不会影响数据的访问，但是没有了数据冗余，可靠性就会降低。为了使数据恢复可靠性，必须在出现磁盘损坏后马上将损坏的磁盘更换并重建镜像卷。镜像卷恢复重建的具体操作步骤如下。

01 打开磁盘管理界面，从图 12-83 可以看出构成镜像卷的两块磁盘中【磁盘 1】正常工作，而另一块显示为【丢失】。右击镜像卷，在弹出的快捷菜单中选择【删除镜像】命令。



图 12-83　镜像卷损坏后的磁盘管理界面

02 弹出【删除镜像】对话框，选中【磁盘】列表中丢失的磁盘，单击【删除镜像】按钮，如图 12-84 所示。

03 弹出【磁盘管理】提示框，单击【是】按钮，如图 12-85 所示。

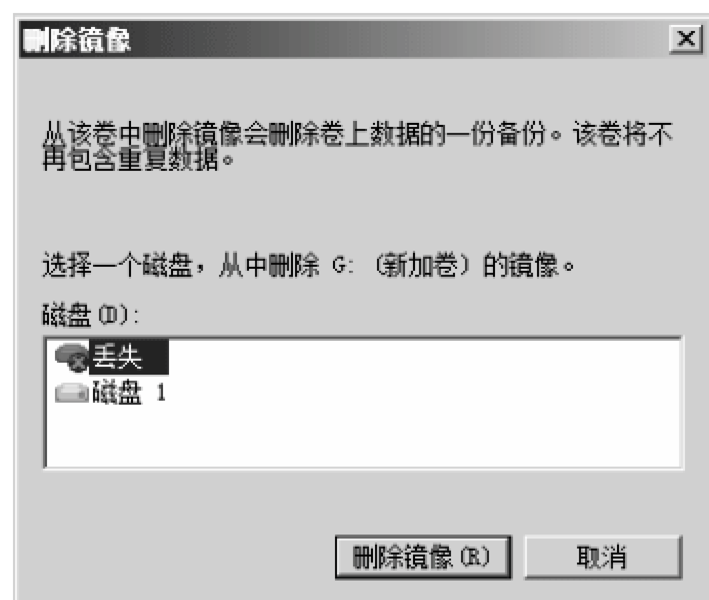


图 12-84 【删除镜像】对话框

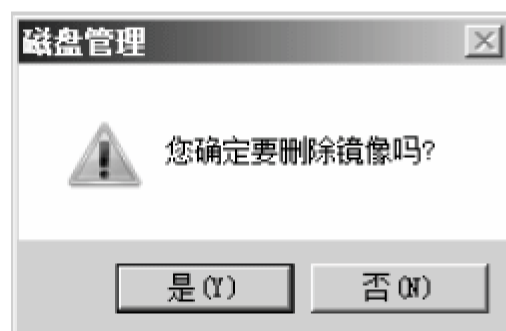


图 12-85 【磁盘管理】提示框

04 丢失的磁盘删除后，另一块磁盘中的卷变成简单卷，右击该简单卷，在弹出的快捷菜单中选择【添加镜像】命令，如图 12-86 所示。



图 12-86 添加新的镜像

05 弹出【添加镜像】对话框，选择可用的新加磁盘，单击【添加镜像】按钮，如图 12-87 所示。

06 返回磁盘管理界面，重建镜像卷成功，如图 12-88 所示。

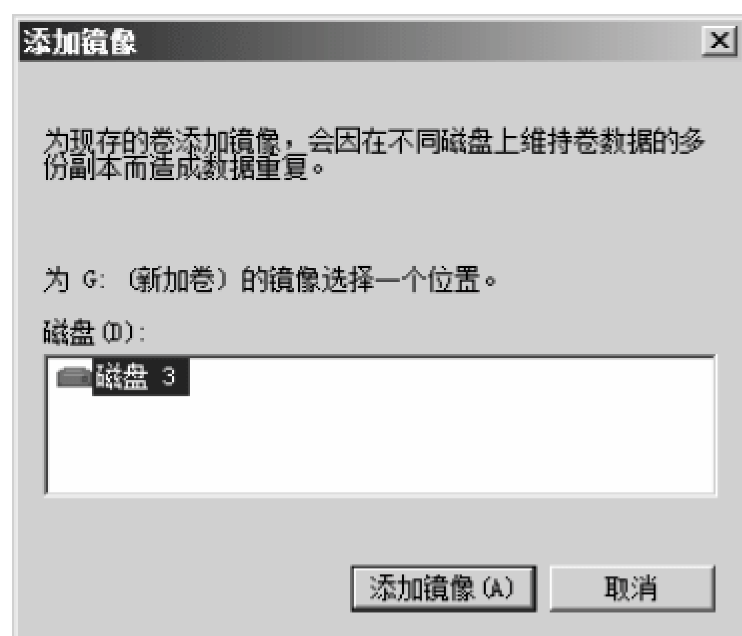


图 12-87 【添加镜像】对话框



图 12-88 镜像卷恢复重建成功

2. RAID-5 卷恢复重建

构成 RAID-5 卷的磁盘最少是三块，且在三块磁盘上使用的空间相同，当其中一块磁盘损坏后，可以使用其他几块磁盘的数据和校验信息找回丢失的数据，但是当构成 RAID-5 卷的磁盘损坏两块以上时，数据将无法恢复。

RAID-5 卷恢复重建的具体操作步骤如下。

01 打开磁盘管理界面，在构成 RAID-5 卷的三块磁盘中【磁盘 1】和【磁盘 2】正常，另外一块丢失，并显示“失败的重复”错误信息，右击构成 RAID-5 卷的一个磁盘空间，在弹出的快捷菜单中选择【修复卷】命令，如图 12-89 所示。



图 12-89 RAID-5 卷损坏后的磁盘管理界面

02 弹出【修复 RAID-5 卷】对话框，选择更换的新磁盘，单击【确定】按钮，如图 12-90 所示。

03 弹出【磁盘管理】提示框，由于新加磁盘原来是基本磁盘，需要被转换为动态磁盘才可用，单击【是】按钮，如图 12-91 所示。



图 12-90 【修复 RAID-5 卷】对话框

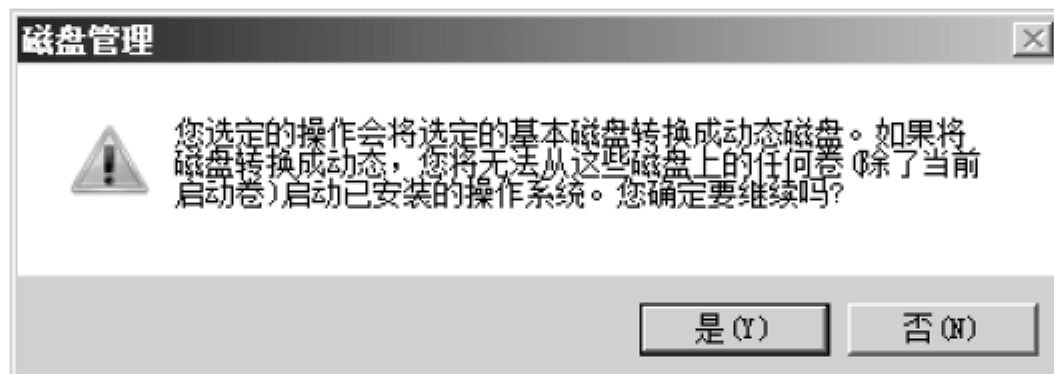


图 12-91 【磁盘管理】提示框

04 返回磁盘管理界面，RAID-5 卷恢复重建成功，并显示为“状态良好”，如图 12-92 所示。



图 12-92 RAID-5 卷恢复重建成功

12.4　专家答疑

（1）做磁盘阵列时，需要多块磁盘，对这些磁盘是否有要求？

答：在做磁盘阵列时，为了保证磁盘阵列稳定运行，建议做磁盘阵列的所有磁盘相同型号，相同容量。

（2）除了使用 RAID 技术实现磁盘阵列外，是否还有其他技术提高磁盘数据的可靠性、稳定性？

答：还有一种技术可以实现和 RAID 相似的功能，是 LVM（ Logical Volume Manager）逻辑卷管理，它是 Linux 环境下对磁盘分区进行管理的一种机制。不适用于挖 Windows 环境。但是该技术在 Linux 服务器中使用非常广泛。

第 13 章　企业 OA 办公自动化系统的维护与管理

随着计算机技术、通信技术和网络技术的发展，工作效率的提高以及公司管理成本的降低越来越依赖于信息化，作为信息化重要组成部分的 OA 系统在办公自动化过程中起到越来越重要的作用。OA 就是采用 Internet/Intranet 技术，基于工作流的概念，使企业内部人员方便快捷地共享信息，高效地协同工作；改变过去复杂、低效的手工办公方式，实现迅速、全方位的信息采集、信息处理，为企业的管理和决策提供科学的依据。一个企业实现办公自动化的程度也是衡量其实现现代化管理的标准之一。

13.1　企业 OA 办公自动化系统概述

网络时代的公司信息化管理需求大大增加，传统的办公模式已经极大的束缚了人的创造力和想象力，埋没了人的智慧和潜能，使员工消耗了大量的时间和精力去手工处理那些繁杂、重复的工作，手工模式日益无法满足新形势下发展的需求，需要使用先进的生产管理工具来提高企业的办公效率。

OA 又叫做办公自动化（Office Automation），就是用来处理企业日常办公事务的管理软件，也称 E-Office，主要可以为企业解决以下问题。

1. 建立企业信息发布平台

在公司内部建立一个有效的信息发布和员工之间交流的平台，使得公司信息和员工思想等能够很好地在企业内部或管理层中得到广泛的传播，使得员工能够及时了解公司的发展状态。

2. 实现工作流程的规范化和自动化

很多企业内部都会有各种各样的流程，如请假流程、出差流程、各种文件审批流程等，这些流程都牵涉到各个部门，为了提高工作效率，解决各个流程之间涉及的部门之间的协同工作问题，可以将流程进行规范化，然后实现工作流程的自动化，以规范各项工作。

3. 实现知识和资产管理的自动化

在传统的手工办公模式下，公司文件和公司各种资产的保存、共享及使用都十分困难，办公

自动化可以实现各种文档和公司资产的自动化管理，通过公共文件柜和网络硬盘的设置，不同的账户具有不同的访问权限，则每个员工可以使用具有相应权限的账户登录 OA 系统，就可以看到或者使用符合员工身份的权限范围内的企业的文件或者公司资产。

4. 辅助协同办公

公司的规模越来越大，员工的数量越来越多，公司不同分支机构、位于不同位置的员工通过 OA 系统能够有效地获得整体的公司信息，提高公司整体的反应速度和决策能力。

13.2　项目实战 1：搭建 OA 办公自动化环境

中国兵器工业信息中心通达科技是一支以协同管理软件研发与实施、ERP 软件研发与咨询、卫星通信服务、网络系统集成为主营业务的高科技团队。通达团队成员均为中国兵器工业信息中心职工。通达 OA（Office Anywhere）网络智能办公系统是适用于企事业单位的通用型网络办公软件，融合了通达科技长期从事管理软件开发的丰富经验与先进技术。该系统采用领先的 B/S（浏览器/服务器）操作方式，使得网络办公不受地域限制。通达 OA 为当前中国最为流行的办公自动化系统之一，本文中讲解的 OA 系统采用从通达 OA 官方网站下载的通达 OA2010 版试用版。

通达 OA 软件的安装过程比较简单，只需要根据提示进行安装即可，安装通达 OA 软件的具体操作步骤如下。

01 双击通达 OA 安装文件，如图 13-1 所示，弹出通达 OA2010 的安装欢迎界面。



图 13-1　通达 OA 安装欢迎界面

02 弹出【欢迎使用通达 OA】对话框，如图 13-2 所示，单击【下一步】按钮。

03 弹出【选择软件安装路径】对话框，单击【浏览】按钮，自定义通达 OA 的安装路径，默认安装路径为“D:/MYOA”，本示例采用默认安装路径，如图 13-3 所示，单击【下一步】按钮。

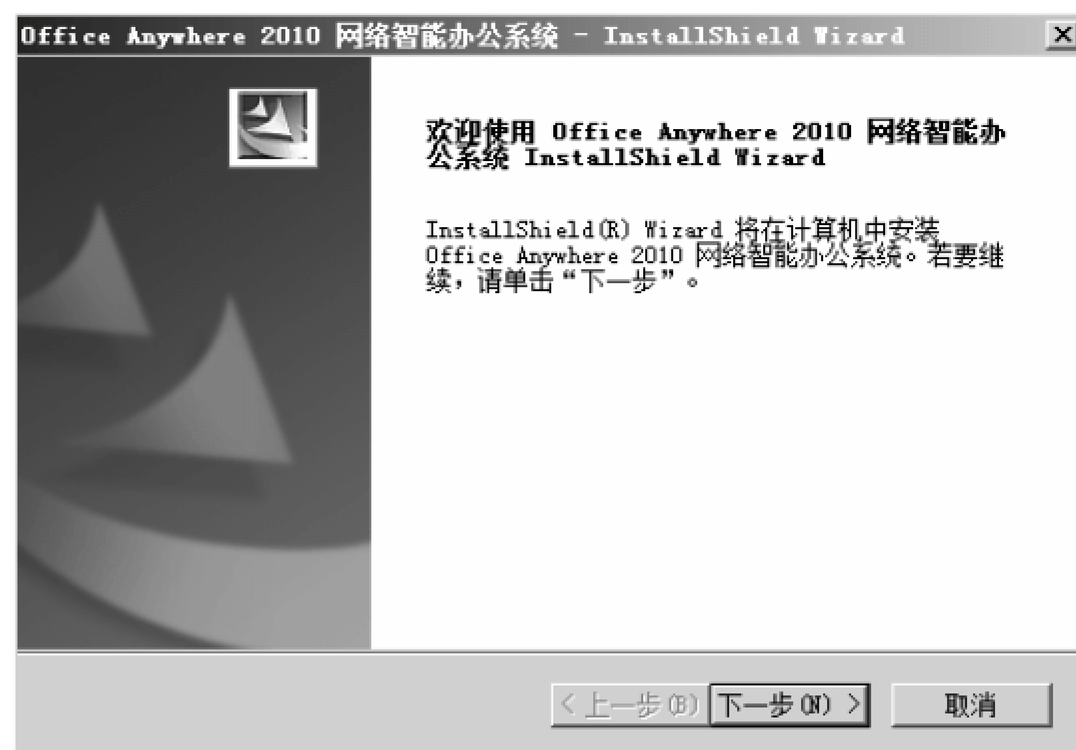


图 13-2 欢迎使用通达 OA 对话框

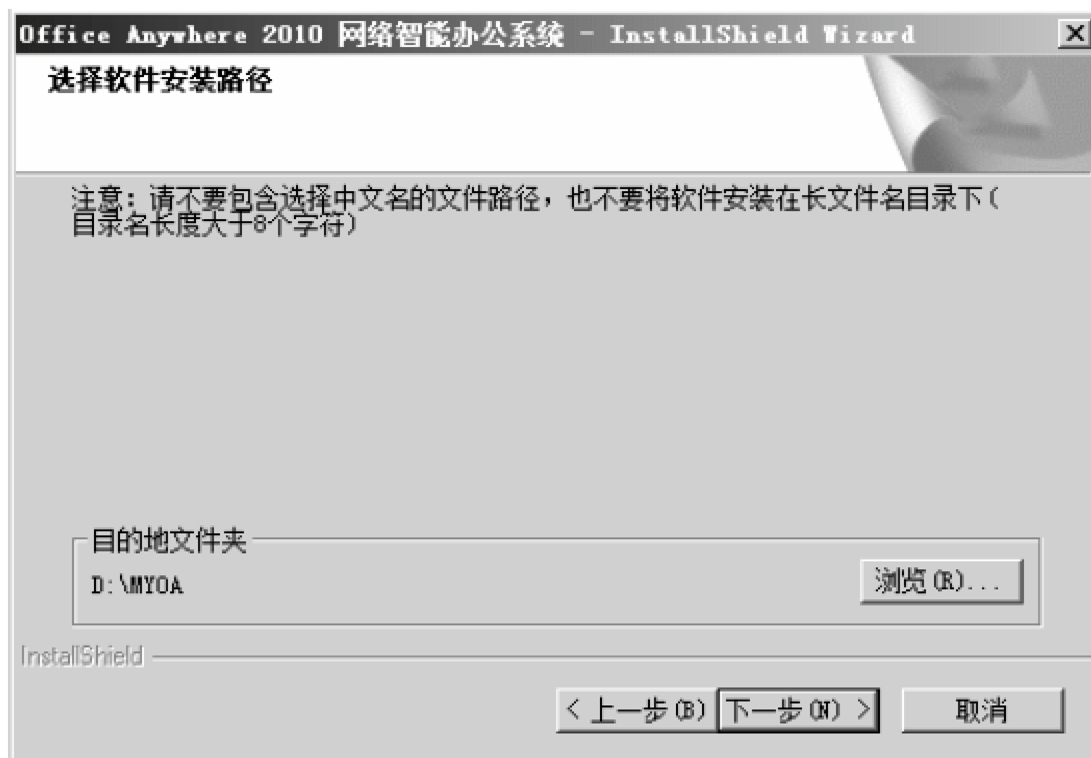


图 13-3 【选择软件安装路径】对话框

04 弹出【可以安装该程序了】对话框，如图 13-4 所示，单击【安装】按钮。

05 如图 13-5 所示，通达 OA2010 网络智能办公系统正在安装，并显示安装进度。

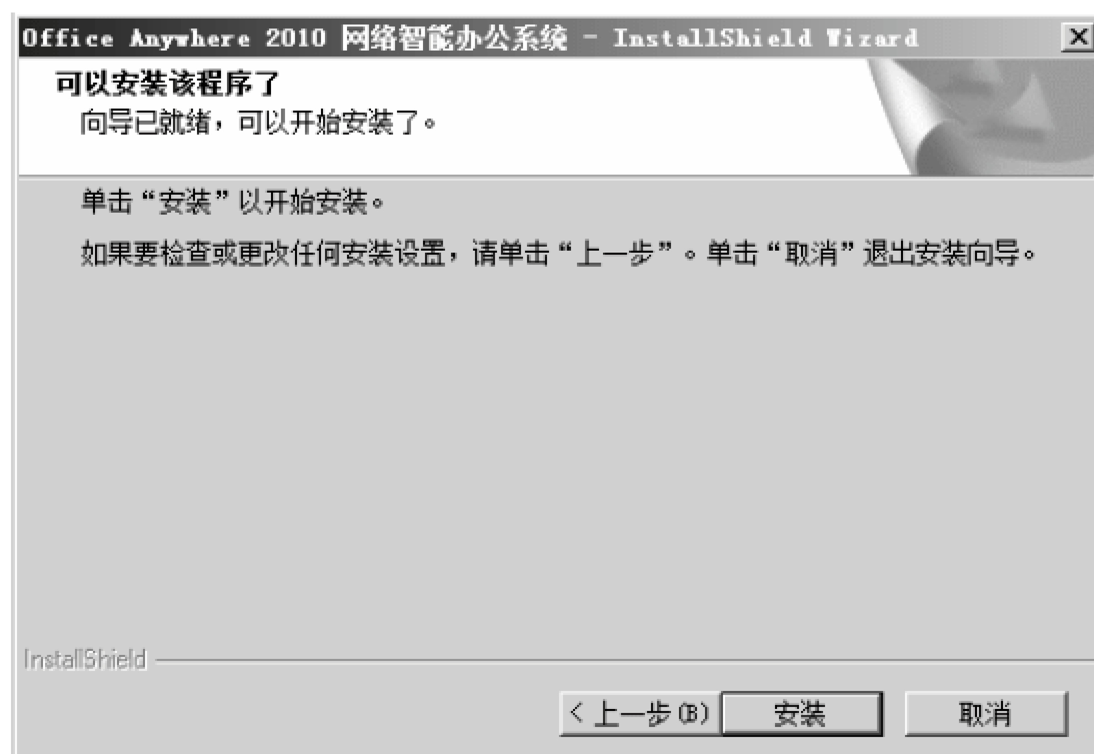


图 13-4 【可以安装该程序了】对话框



图 13-5 通达 OA 安装进度

06 如图 13-6 所示，OA 安装完成后开始进行系统智能配置。

07 弹出 OA 安装完成对话框，如图 13-7 所示，单击【完成】按钮。

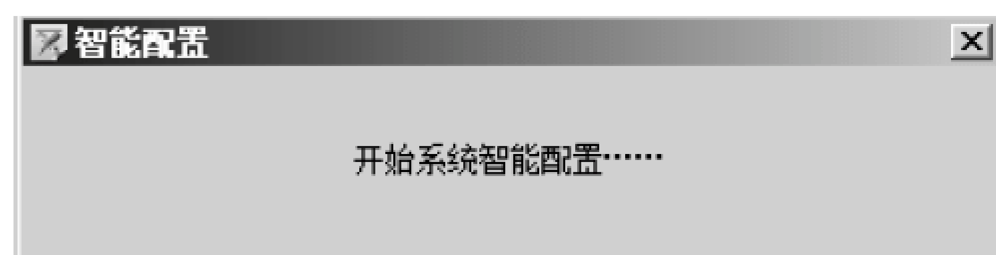


图 13-6 【智能配置】提示框



图 13-7 OA 安装完成对话框

08 弹出【Office Anywhere 服务配置】对话框，如图 13-8 所示，单击【端口检测】按钮。

09 弹出 NetWork 提示框，表示端口 80 可以使用，如图 13-9 所示，单击【确定】按钮。

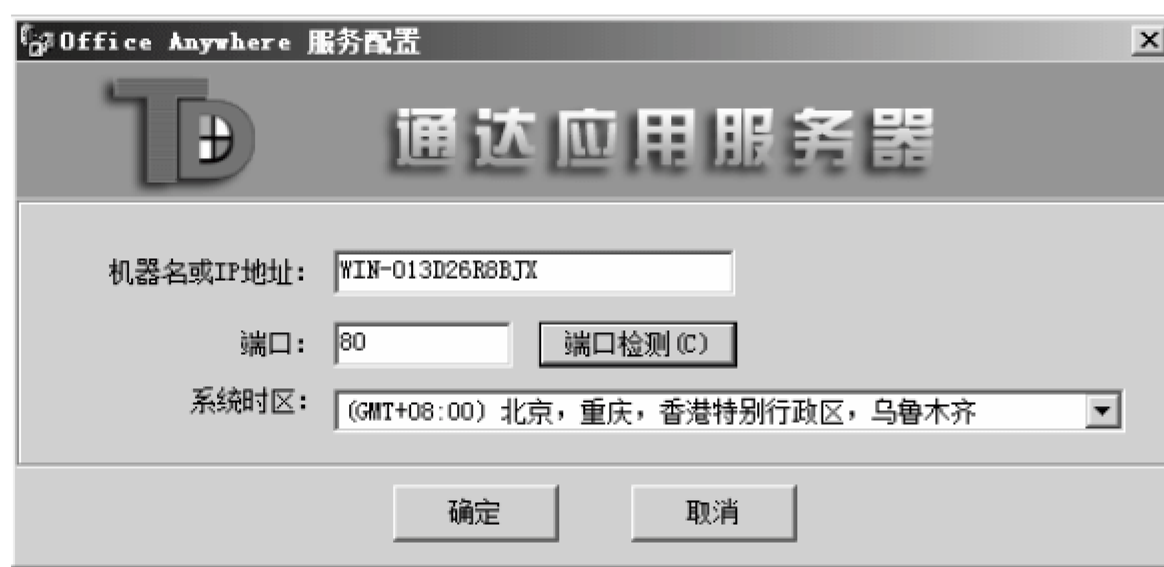


图 13-8　【Office Anywhere 服务配置】对话框



图 13-9　【NetWork】提示框

10 返回至【Office Anywhere 服务配置】对话框，单击【确定】按钮，完成通达 OA2010 的安装。

11 弹出【配置完成】提示框，如图 13-10 所示，单击【确定】按钮。

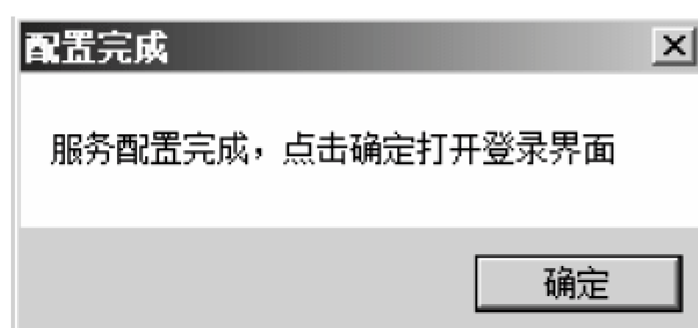


图 13-10　【配置完成】提示框

12 弹出通达 OA2010 的登录界面，如图 13-11 所示，表示通达 OA 安装成功。



图 13-11　通达 OA2010 的登录界面

13.3　项目实战 2：配置管理 OA 系统，实现办公自动化

实现 OA 办公自动化首先需要对公司组织架构和员工信息进行设置，如图 13-12 所示，本实例

以尖峰科技有限公司实际情况为案例进行 OA 系统建设与管理。

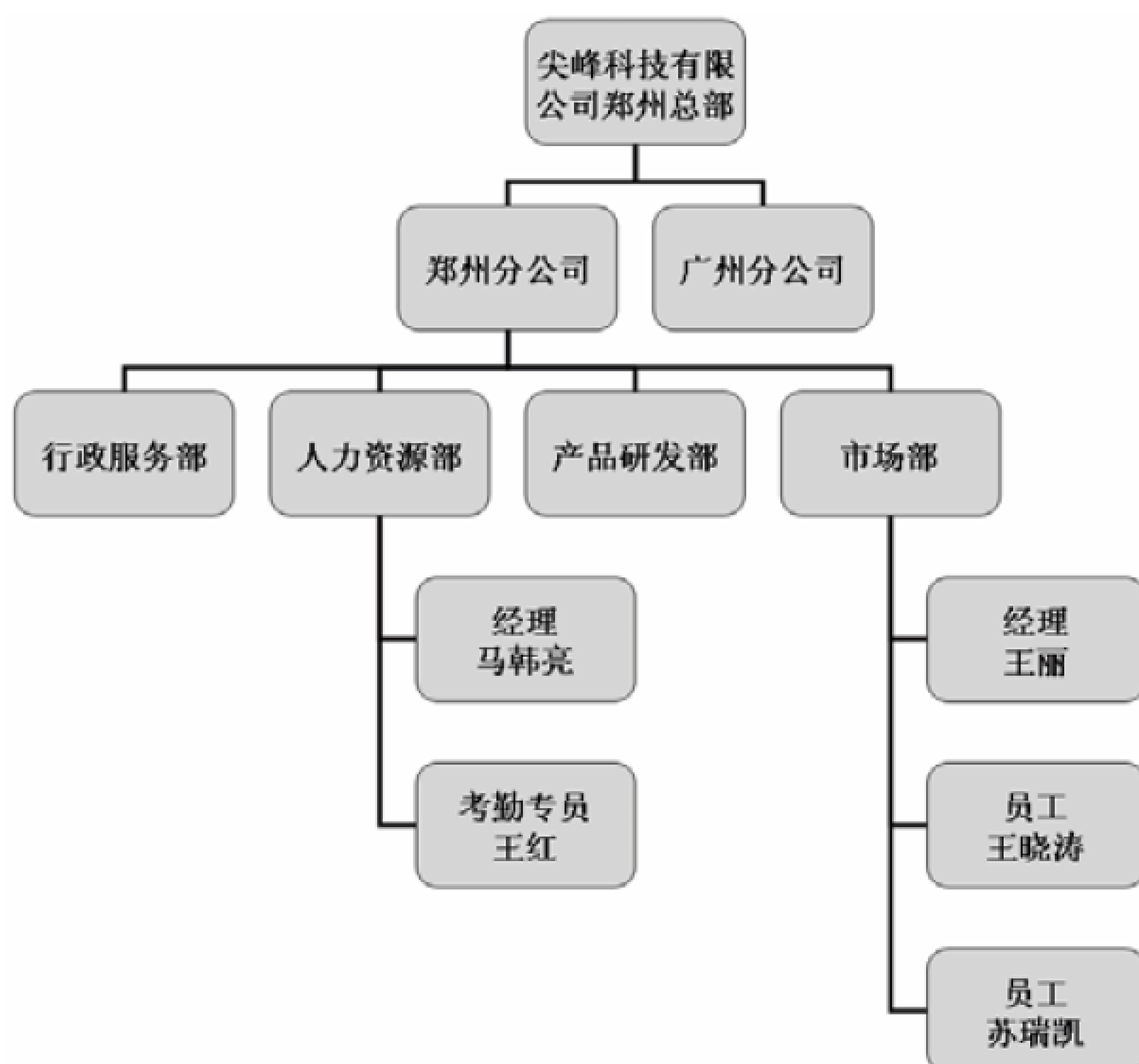


图 13-12　尖峰科技有限公司组织架构图

13.3.1　实现员工权限设置管理

OA 办公自动化系统中用户的权限是以角色来进行限制的。在新建用户之前首先根据公司员工的职位和岗位职责不同，将公司员工分成几类角色，然后以这些角色为模板建立员工账户。建立角色的具体操作步骤如下。

01 打开 IE 浏览器，如图 13-13 所示，在地址栏里输入“http://192.168.1.200”，其中“192.168.1.200”为通达 OA 服务器的 IP 地址，按 Enter 键。



图 13-13　登录 OA 服务器

02 打开通达 OA2010 登录界面，在【用户名】和【密码】文本框中分别输入 OA 管理员的账户和密码，通达 OA 管理员的默认用户名为“admin”，管理员的默认密码为空，如图 13-14 所示，在【用户名】文本框中输入“admin”，单击【登录】按钮。



图 13-14　通达 OA2010 登录界面

03 打开管理员 OA【个人桌面】操作界面，如图 13-15 所示，选择【菜单】➢【系统管理】➢【组织机构设置】➢【角色与权限管理】选项。



图 13-15　管理员 OA【个人桌面】操作界面

04 打开通达 OA 超级管理员登录页面，在【请输入超级密码】文本框中输入超级管理员的密码，超级管理员的密码默认为空，如图 13-16 所示，单击【确定】按钮。

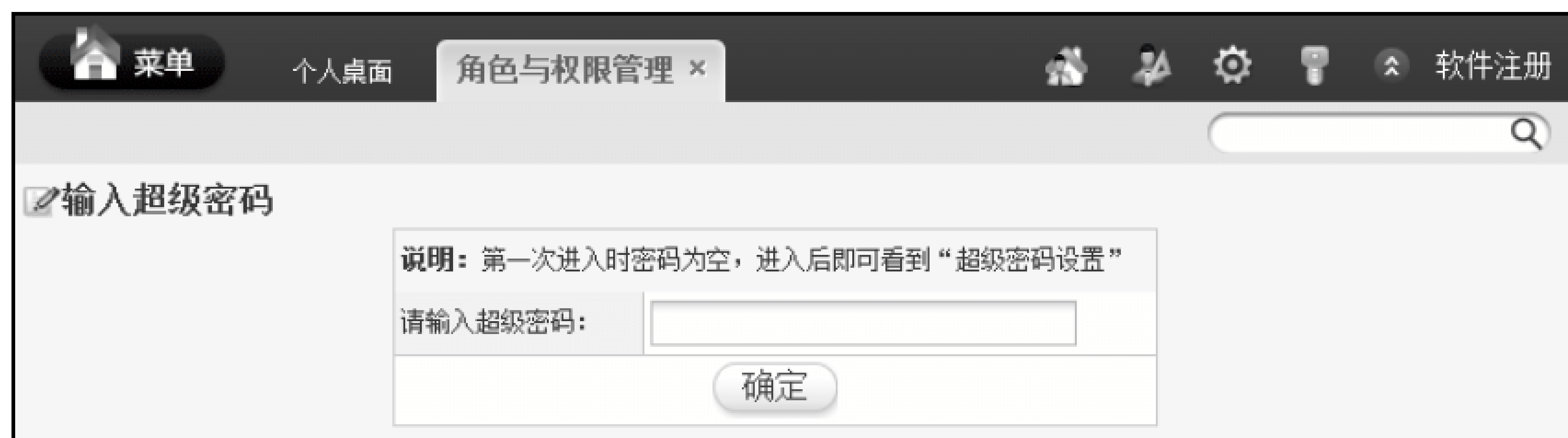


图 13-16　通达 OA 超级管理员登录页面

05 打开【角色与权限管理】界面，默认情况下通达 OA 将账户的角色分为总经理、部门经理、OA 管理员、财务主管、职员等 5 种，如果需要更改现有角色的权限，单击角色名后面的【设置权限】链接。本实例更改部门经理的权利，如图 13-17 所示，单击【部门经理】角色后面的【设

置权限】链接。



图 13-17 【角色与权限管理】界面

06 打开部门经理的权限设置界面，如图 13-18 所示，若需添加权利则选中相关权利前面的复选框，若需删除权限则不选中相关权限前面的复选框，单击【确定】按钮完成权限的更改。

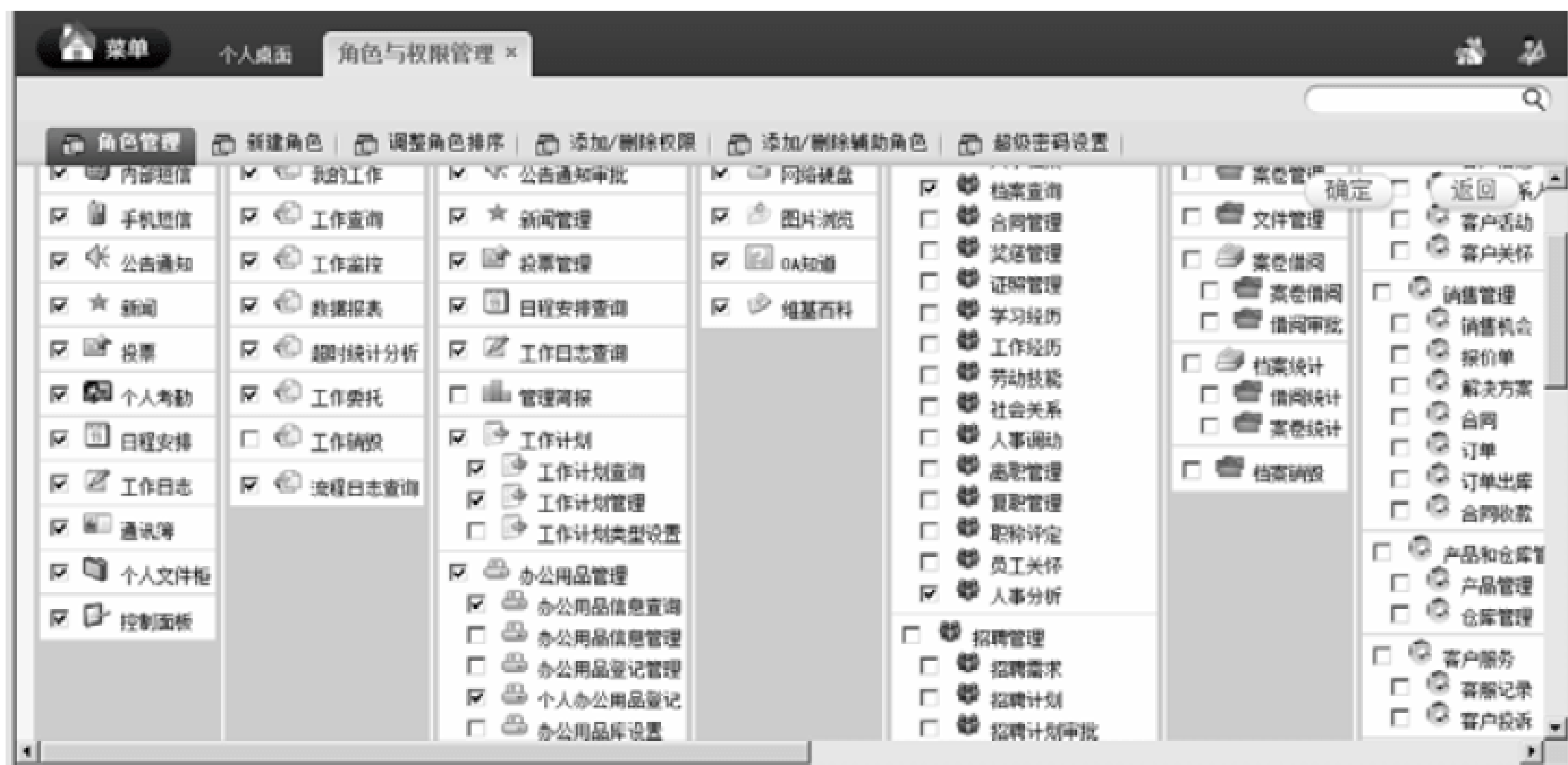


图 13-18 权限设置界面

07 返回至【角色与权限管理】界面，如果需要添加新的角色，单击【新建角色】标签。打开【新建角色】选项卡，在【角色排序号】和【角色名称】文本框中分别输入角色序列号和角色名称，如图 13-19 所示，本实例中输入角色排序号为“11”，角色名称为“考勤专员”，单击【确定】按钮。

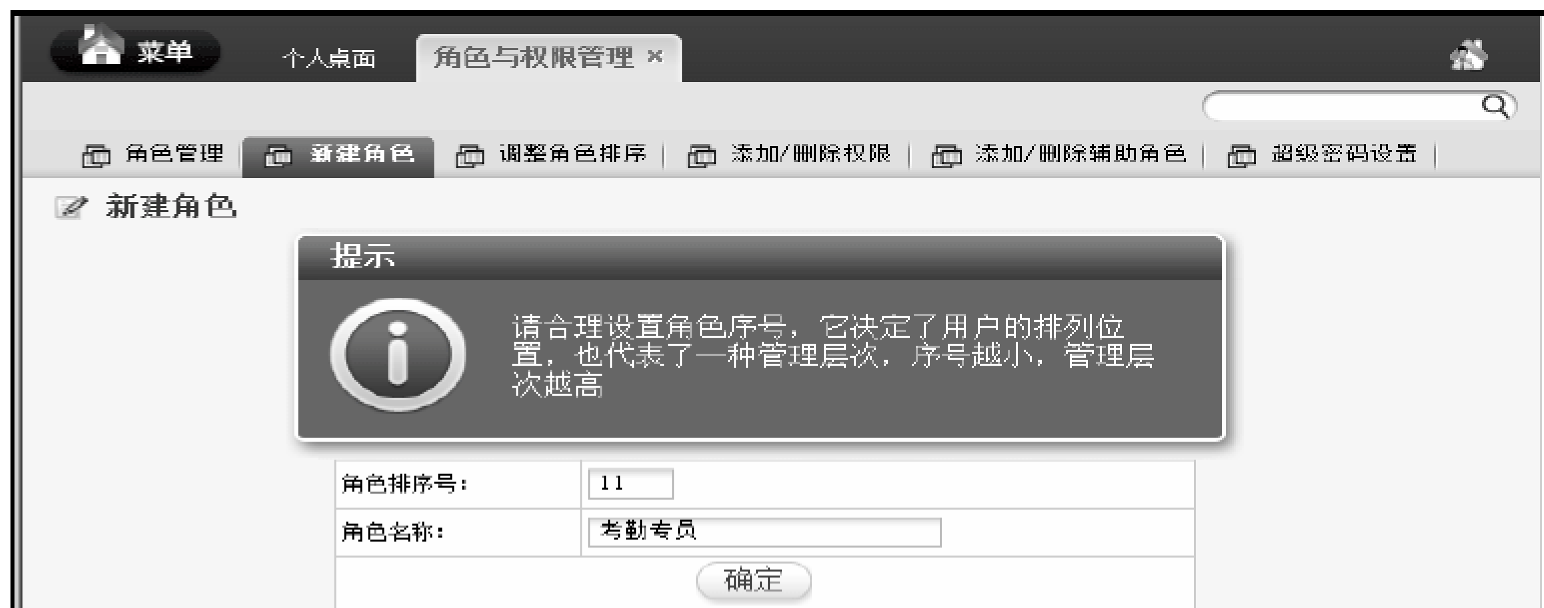


图 13-19 【新建角色】选项卡

08 打开【管理角色】页面，单击【考勤专员】角色后面的【设置权限】链接。

09 打开角色权限设置界面，选中角色【考勤专员】具有的相关权利复选框，如图 13-20 所示，本实例选中考勤管理相关权利，单击【确定】按钮。



图 13-20　角色权限设置界面

10 返回至【管理角色】页面，新的角色创建完成。

13.3.2　实现 OA 账户管理

通达 OA 的角色建立完成后，就可以进行 OA 账户的建立，建立通达 OA 账户的具体操作步骤如下。

01 打开 IE 浏览器，在地址栏中输入“http://192.168.1.200”，其中“192.168.1.200”为通达 OA 服务器的 IP 地址，按 Enter 键。

02 打开通达 OA2010 登录界面，在【用户名】和【密码】文本框中分别输入 OA 管理员的账户和密码，通达 OA 管理员的默认用户名为“admin”，管理员的默认密码为空，在【用户名】文本框中输入“admin”，单击【登录】按钮。

03 打开管理员 OA【个人桌面】操作界面，选择【菜单】➢【系统管理】➢【组织机构设置】➢【单位管理】选项。

04 打开【单位管理】界面，在【单位名称】、【电话】、【传真】、【邮编】、【地址】、【网站】和【电子信箱】等文本框中分别输入企业相关信息，单击页面最下方的【保存单位设置】按钮，如图 13-21 所示。

05 返回至通达 OA2010 操作界面，选择【菜单】➢【系统管理】➢【组织机构设置】➢【部门管理】选项。



图 13-21 【单位管理】界面

06 打开【部门管理】界面，在【部门排序号】、【部门名称】、【电话】、【传真】等文本框中输入公司总部相关信息，单击【新建】按钮，如图 13-22 所示。



图 13-22 【部门管理】界面

07 在【部门排序号】、【部门名称】、【电话】、【传真】等文本框中分别输入郑州分公司相关信息，在【上级部门】下拉列表框中选择【郑州总部】，单击【新建】按钮，如图 13-23 所示。

08 在【部门排序号】、【部门名称】、【电话】、【传真】等文本框中输入【广州分公司】相关信息，在【上级部门】下拉列表框中选择【郑州总部】，单击【新建】按钮，如图 13-24 所示。

图 13-23　新建郑州分公司部门

图 13-24　新建广州分公司部门

09 在【部门排序号】、【部门名称】、【电话】、【传真】等文本框中输入行政服务部相关信息，在【上级部门】下拉列表框中选择【郑州分公司】，单击【新建】按钮，如图 13-25 所示。

10 依据上述步骤依次建立郑州分公司的【人力资源部】、【产品研发部】、【市场部】等部门，在新建部门页面的左侧显示创建好的部门列表，如图 13-26 所示。

图 13-25　新建行政服务部部门

图 13-26　部门列表

11 在通达 OA2010 操作界面中选择【菜单】➢【系统管理】➢【组织机构设置】➢【用户管理】选项。

12 打开【用户管理】界面，如图 13-27 所示，选择左侧【郑州总部】选项。

13 打开【新建用户】界面，如图 13-28 所示，单击【新建用户】按钮。



图 13-27 【用户管理】界面



图 13-28 【新建用户】界面

14 打开新建用户信息设置页面，如图 13-29 所示，在【用户基本信息】选项域中，在【用户名】文本框中输入人力资源部员工“王红”的登录用户名“wanghong”，在【真实姓名】文本框中输入姓名为“王红”，在【主角色】下拉列表框中选择【职员】。选择【指定辅助角色】选项，然后单击【辅助角色】文本框后面的【添加】链接。

15 弹出【选择角色】对话框，本实例中人力资源员工“王红”同时具有“职员”和“考勤专员”的的权利，如图 13-30 所示，选择【考勤专员】选项，单击【确定】按钮。返回用户信息设置页面，在【部门】下拉列表框中选择【人力资源部】。



图 13-29 新建用户信息设置页面



图 13-30 【选择角色】对话框

16 在【用户可自定义选项】选项域的【密码】文本框中输入账户“wanghong”的密码，本实例中密码为空。如图 13-31 所示，单击【新建】按钮。

17 弹出【用户增加成功】提示框，如图 13-32 所示，单击【继续新建用户】按钮。

图 13-31　用户可自定义选项



图 13-32　用户增加成功

18 打开用户信息设置页面，在【用户名】文本框中输入市场部经理“王丽”的登录用户名“wangli”，在【真实姓名】文本框中输入姓名为“王丽”，在【主角色】下拉列表框中选择【部门经理】，在【部门】下拉列表框中选择【市场部】，如图 13-33 所示。

19 如图 13-34 所示，在【用户可自定义选项】选项域的【密码】文本框中输入账户“wangli”的密码，本实例密码为空，单击【新建】按钮。

图 13-33　用户信息设置页面

图 13-34　用户可自定义选项

20 根据上述步骤依次添加市场部员工王晓涛、市场部员工苏瑞凯、人力资源部经理马韩亮等员工账号，如图 13-35 所示。



图 13-35 【用户管理】页面

13.3.3 实现通信与信息共享

通达 OA 自动办公系统实现通信与信息共享的手段主要是邮件和短消息，具体的操作步骤如下。

01 打开通达 OA2010 登录界面，如图 13-36 所示，在【用户名】文本框中输入“wanghong”，密码为空，单击【登录】按钮。

02 打开员工王红的 OA【个人桌面】操作界面，如图 13-37 所示，单击【邮件】图标。



图 13-36 通达 OA2010 登录界面



图 13-37 员工王红的 OA【个人桌面】操作界面

03 打开员工王红的 OA【电子邮件】页面，如图 13-38 所示，单击【写信】按钮。



图 13-38 【电子邮件】页面

04 打开员工“王红”的 OA【写邮件】页面，如图 13-39 所示，单击【收件人】文本框后面的【添加】按钮。



图 13-39　【写邮件】页面

05 弹出【选择人员】对话框，如图 13-40 所示，选择【系统管理员】，然后单击【确定】按钮。



图 13-40　【选择人员】页面

06 返回至员工“王红”的 OA【电子邮件】页面，在【邮件主题】和【邮件内容】文本框中分别输入要发送邮件的主题和内容，如图 13-41 所示，选中【发送事务提醒消息】复选框，单击【立即发送】按钮。

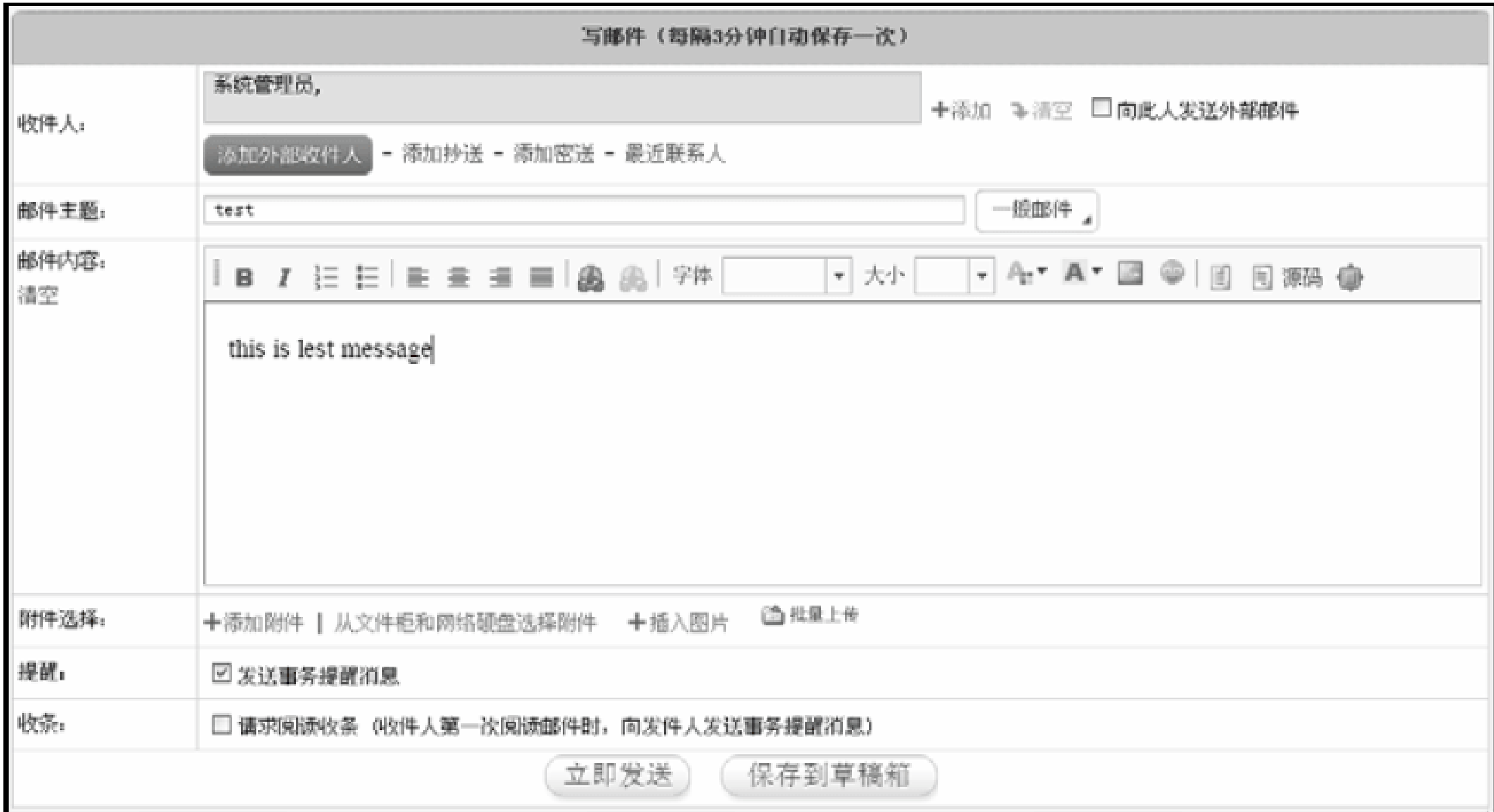


图 13-41　【电子邮件】页面

07 弹出邮件发送成功提示，如图 13-42 所示，表明发送邮件成功。



图 13-42　邮件发送成功提示

08 打开通达 OA2010 登录界面，如图 13-43 所示，在【用户名】文本框中输入“Admin”，密码为空，单击【登录】按钮。

09 打开系统管理员的 OA【个人桌面】操作界面，弹出新消息提示框，如图 13-44 所示，单击【打开】按钮。



图 13-43　【通达 OA2010】登录界面

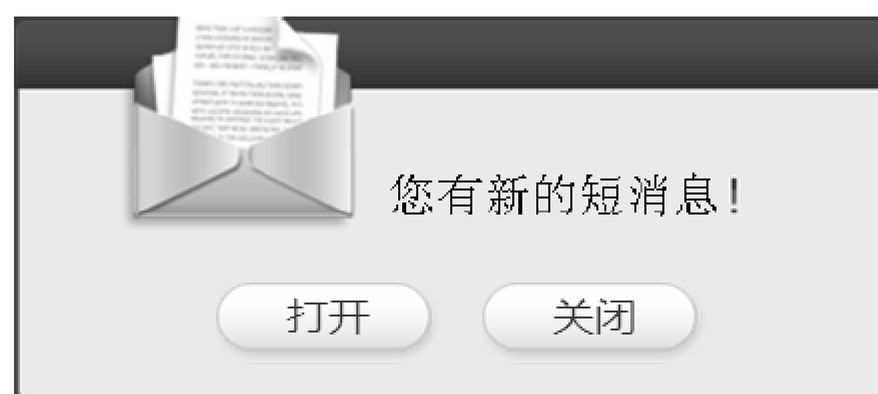


图 13-44　新消息提示框

10 弹出【消息盒子】提示框，如图 13-45 所示，提示有新邮件，单击【查看详情】超链接。



图 13-45　【消息盒子】提示框

11 如图 13-46 所示，弹出【邮件正文】页面。



图 13-46 【邮件正文】页面

13.3.4 企业新闻和公告管理

通达 OA 办公自动化系统可以实现企业新闻的发布和企业公告的管理，具体的操作步骤如下。

1. 添加新闻与公告管理角色权限

01 打开通达 OA2010 登录界面，通达 OA 管理员的默认用户名为“admin”，管理员的默认密码为空，如图 13-47 所示，在【用户名】文本框中输入“admin”，单击【登录】按钮。

02 打开通达 OA【个人桌面】界面，选择【菜单】➢【系统管理】➢【组织机构设置】➢【角色与权限管理】选项。



图 13-47 通达 OA2010 登录界面

03 打开【角色与权限管理】界面，在【请输入超级密码】文本框中输入超级管理员的密码，超级管理员的密码默认为空，单击【确定】按钮。

04 进入【角色与权限管理】的超级管理员管理界面，如图 13-48 所示，选择【新建角色】页面，显示新建角色的提示信息，在【角色排序号】和【角色名称】文本框中分别输入相关信息，单击【确定】按钮。



图 13-48 【新建角色】页面

05 新角色添加成功，单击【新闻与通告管理】角色后面的【设置权限】链接，如图 13-49 所示。



图 13-49 【角色与权限管理】界面

06 打开【编辑角色权限】页面，选中【公告通知管理】、【公告通知审批】和【新闻管理】等复选框，单击【确定】按钮，如图 13-50 所示。



图 13-50 【编辑角色权限】页面

07 角色权限设置成功，选择【菜单】➢【系统管理】➢【组织机构设置】➢【用户管理】选项。

08 打开【用户管理】页面，选择左侧【郑州总部】选项，如图 13-51 所示。



图 13-51　【用户管理】页面

09 如图 13-52 所示，单击【新建用户】按钮。



图 13-52　新建用户

10 打开【新建用户】页面，分别填入行政服务部员工“冯亮”的相关信息，在【主角色】下拉列表框中选择【职员】角色，选择【指定辅助角色】选项，然后单击【辅助角色】文本框后面的【添加】按钮，如图 13-53 所示。

11 打开【选择角色】对话框，选择【新闻与通告管理】角色，如图 13-54 所示，单击【确定】按钮。



图 13-53　【新建用户】页面



图 13-54　【选择角色】页面

12 返回至【新建用户】页面，在【部门】下拉列表框中选择郑州分公司的【行政服务部】部门，单击【新建】按钮。

13 弹出用户增加成功提示，单击【关闭】按钮。

2. 发布新闻和公告

01 打开通达 OA 2010 登录界面，在【用户名】和【密码】文本框中分别输入行政服务部员工“冯亮”的用户名和密码，如图 13-55 所示，单击【登录】按钮。

02 打开员工“冯亮”的 OA【个人桌面】操作界面，如图 13-56 所示，选择【菜单】➢【行政办公】➢【公告通知管理】命令。



图 13-55　通达 OA 2010 登录界面



图 13-56　【行政办公】菜单

03 打开【公告通知管理】页面，如图 13-57 所示，单击【新建公告】选项。



图 13-57　【公告通知管理】页面

04 打开【新建公告通知】页面，在【选择公告类型】文本框中输入公告标题“停电通知”，单击【按部门发布】文本框后面的【添加】选项，如图 13-58 所示。



图 13-58　【新建公告通知】页面

05 打开【选择部门】对话框，选择需要查看该通告的部门，本实例中希望郑州分公司所有部门人员查看该条公告，如图 13-59 所示，选中【郑州分公司】复选框，单击【确定】按钮。



图 13-59　【选择部门】对话框

06 返回至【新建公告通知】页面，选中【使用内部短信提醒】复选框，在下面公告通知内容文本框中输入相关公告通知，如图 13-60 所示，单击【发布】按钮。



图 13-60　发布公告

07 显示公告发布成功提示，图 13-61 所示，表示公告发布成功。

08 选择【菜单】➢【行政办公】➢【新闻管理】命令。



图 13-61　公告发布成功提示

09 打开【新闻管理】页面，如图 13-62 所示，单击【新建新闻】标签。



图 13-62 【新闻管理】页面

10 打开【新建新闻】页面，如图 13-63 所示，在【选择新闻类型】文本框中输入新闻的标题，单击【按人员或角色发布】标签。



图 13-63 【新建新闻】页面

11 如图 13-64 所示，选择需要查看本新闻的人员或者角色，本实例要求所有职员角色的员工查看本新闻，单击【按角色发布】文本框后面的【添加】按钮。

12 打开【选择角色】对话框，选择【职员】角色，表示只有【职员】角色的用户才可以查看本条新闻，如图 13-65 所示，单击【确定】按钮。



图 13-64 指定具有新闻查看权限的对象



图 13-65 选择角色

13 返回至【新建新闻】页面，选中【使用内部短信提醒】复选框，在下面新闻编辑文本框中输入新闻具体内容，如图 13-66 所示，单击【发布】按钮。



图 13-66　发布新闻

14 显示新闻发布成功提示，如图 13-67 所示。



图 13-67　新闻发布成功提示

3. 用户查看新闻和公告

01 打开通达 OA2010 登录界面，在【用户名】和【密码】文本框中分别输入市场部员工“王晓涛”的用户名和密码，如图 13-68 所示，单击【登录】按钮。

02 打开员工“王晓涛”的 OA【个人桌面】操作界面，弹出新短消息提醒，单击【打开】按钮。



图 13-68　通达 OA2010 登录界面

03 弹出【消息盒子】对话框，如图 13-69 所示，单击【公告通知】右侧的【查看详情】选项。



图 13-69 【消息盒子】对话框

04 弹出【查看公告通知】窗口，如图 13-70 所示，显示公告具体内容。单击【关闭】按钮，关闭公告。

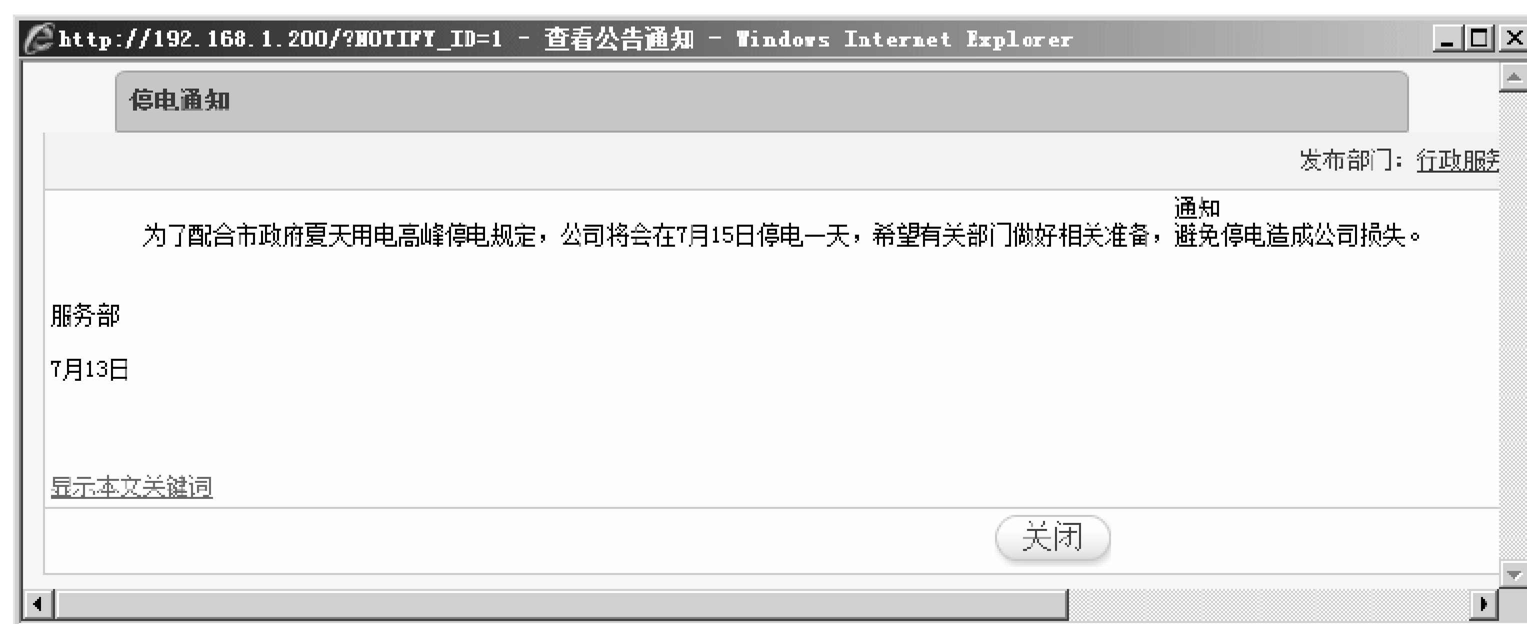


图 13-70 【查看公告通知】窗口

05 返回至【消息盒子】对话框，如图 13-71 所示，单击【新闻】右侧的【查看详情】链接。

06 打开新闻查看页面，图 13-72 所示，可以看到新闻具体内容。





图 13-71 【消息盒子】对话框

图 13-72 新闻查看页面

13.3.5　实现企业信息自由交流

通达 OA 通过投票区的建立和讨论区的建立实现公司内部信息交流的自由，具体的操作步骤如下。

1. 投票区的建立

01 弹出通达 OA2010 登录界面，在【用户名】文本框中输入“admin”，管理员的默认密码为空，单击【登录】按钮。

02 打开管理员 OA【个人桌面】界面，选择【菜单】➢【行政办公】➢【投票管理】命令。

03 打开【投票管理】页面，如图 13-73 所示，单击【新建投票】标签。



图 13-73　【投票管理】页面

04 打开【新建投票】页面，在【标题】文本框中输入投票标题为“内部员工谈恋爱利大还是弊大”，如图 13-74 所示，单击【发布范围（部门）】文本框后面的【添加】按钮。

图 13-74　【新建投票】页面

05 弹出【选择部门】对话框，选择拥有权力进行投票的部门人员。本实例中郑州分公司所有部门员工都有权力进行投票，如图 13-75 所示，选中【郑州分公司】复选框，单击【确定】按钮。



图 13-75 【选择部门】对话框

06 返回至【新建投票】页面，如图 13-76 所示，在【类型】下拉列表框中选择【单选】，在【查看投票结果】下拉列表框中选择【投票后允许查看】，选中【允许匿名投票】复选框，单击【保存】按钮。



图 13-76 【新建投票】页面

07 弹出【投票保存成功】提示框，表示投票保存成功，如图 13-77 所示，单击【添加投票项目】按钮。



图 13-77 【投票保存成功】提示框

08 打开【投票项目管理】页面，如图 13-78 所示，在【添加项目】文本框中输入投票项目为“利大，有利于员工稳定和部门间交流”，单击【添加】按钮。



图 13-78　【投票项目管理】页面

09 返回至【投票项目管理】页面，如图 13-79 所示，在【添加项目】文本框中输入投票项目为“弊大，容易形成小集团思想不利于提高工作效率”，单击【添加】按钮。



图 13-79　添加第二个项目

10 返回至【投票项目管理】页面，如图 13-80 所示，在【添加项目】文本框中输入投票项目为“有利也有弊主要看当事人如何选择”，单击【添加】按钮。



图 13-80　添加第三个项目

11 返回至【投票项目管理】页面，如图 13-81 所示，单击【返回】按钮。



图 13-81　添加完成所有项目

12 返回至【投票管理】页面，如图 13-82 所示，单击【立即发布】链接。



图 13-82　发布投票

13 弹出【来自网页的消息】提示框，如图 13-83 所示，单击【确定】按钮。

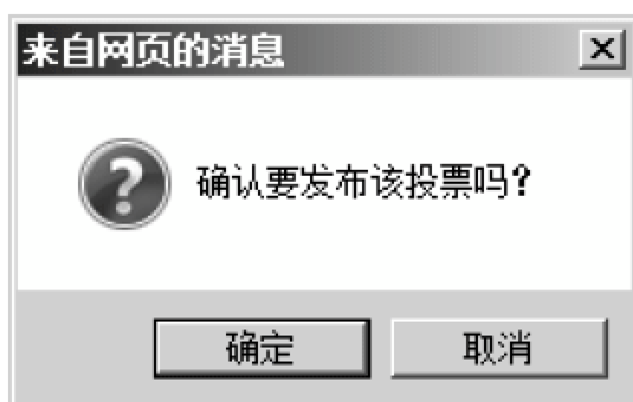


图 13-83　【来自网页的消息】提示框

14 返回至【投票管理】页面，如图 13-84 所示，投票区建立完成。



图 13-84　投票区建立完成

15 员工进行投票。如图 13-85 所示，郑州分公司人力资源部员工“王红”进行 OA 登录。

16 打开员工“王红”的 OA【个人桌面】操作界面，如图 13-86 所示，单击【投票】图标。



图 13-85　OA 登录页面



图 13-86　【个人桌面】操作界面

17 弹出【投票】窗口，如图 13-87 所示，单击【内部员工谈恋爱利大还是弊大】链接。



图 13-87 【投票】窗口

18 打开投票页面，根据实际情况选中 A、B、C 三个单选按钮中的一个，如图 13-88 所示，本实例中选中 C 单选按钮，单击【投票】按钮。



图 13-88 投票页面

19 显示【投票完成】提示，单击【返回】按钮，完成投票，如图 13-89 所示。



图 13-89 【投票完成】提示

20 打开【投票结果】页面，如图 13-90 所示，可以看到投票结果。



图 13-90 【投票结果】页面

2. 话题讨论区的建立

01 打开通达 OA2010 登录界面，在【用户名】对话框中输入 “admin” ，管理员的默认密码为空，单击【登录】按钮。

02 打开管理员的 OA【个人桌面】操作界面，如图 13-91 所示，选择【菜单】➢【系统管理】

➢【信息交流设置】➢【讨论区设置】选项。



图 13-91 【讨论区设置】选项

03 打开【讨论区设置】页面，单击【新建讨论区】按钮，如图 13-92 所示。



图 13-92 【讨论区设置】页面

04 打开【新建讨论区】页面，如图 13-93 所示，分别在相应文本框中输入讨论区相关内容，单击【开放范围（部门）】文本框后面的【添加】按钮。

排序号:	1
讨论区名称:	关于春游地点的讨论
讨论区简介:	公司定于4月5日组织全体员工进行春游，大家可以对于春游的地点进行建
开放范围(部门):	+添加 清空
开放范围(角色):	+添加 清空
开放范围(人员):	+添加 清空
版主:	+添加 清空
是否允许匿名发帖:	允许
提醒:	使用内部短信提醒
	保存 返回

图 13-93 【新建讨论区】页面

05 弹出【选择部门】对话框，如图 13-94 所示，选中【郑州分公司】复选框，单击【确定】按钮。



图 13-94　【选择部门】对话框

06 返回至【新建讨论区】页面，在【是否允许匿名发帖】下拉列表框中选择【允许】，如图 13-95 所示，选中【使用内部短信提醒】复选框，单击【保存】按钮。



图 13-95　【新建讨论区】页面

07 返回至【讨论区设置】页面，如图 13-96 所示，可以看到新建的讨论区。



图 13-96　【讨论区设置】页面

08 员工登录 OA 进行话题讨论。如图 13-97 所示，市场部员工“王丽”进行 OA 登录。

09 打开员工“王丽”的 OA【个人桌面】操作界面，弹出新短消息提示框，单击【打开】按钮。



图 13-97 OA 登录页面

10 弹出【消息盒子】对话框，如图 13-98 所示，单击【查看详情】链接。



图 13-98 【消息盒子】对话框

11 弹出【讨论区列表】页面，如图 13-99 所示，单击【关于春游地点的讨论】链接。



图 13-99 【讨论区列表】页面

12 弹出【讨论区】页面，如图 13-100 所示，单击【发帖】按钮。



图 13-100 【讨论区】页面

13 弹出【编辑文章】页面，如图 13-101 所示，分别填入讨论相关内容，选中【提醒全部有权限人员】复选框，单击【保存】按钮。

图 13-101　【编辑文章】页面

14 返回至【讨论区】窗口，如图 13-102 所示，可以看到关于这个话题的所有讨论。

图 13-102　【讨论区】窗口

13.3.6　实现文件管理与共享

为了方便公司文件的管理与共享，通达 OA 通过建立公共文件柜和网络硬盘来实现。本文重点讲解公共文件柜的建立与管理。建立公共文件柜的具体操作步骤如下。

01 打开通达 OA2010 登录界面，在【用户名】对话框中输入“admin”，管理员的默认密码为空，单击【登录】按钮。

02 弹出管理员 OA【个人桌面】操作界面，如图 13-103 所示，选择【菜单】➢【系统管理】➢【知识管理设置】➢【公共文件柜设置】命令。



图 13-103　【公共文件柜设置】选项

03 打开【公共文件柜设置】页面，如图 13-104 所示，单击【新建文件夹】按钮。



图 13-104　【公共文件柜设置】页面

04 打开【新建文件夹】页面，如图 13-105 所示，在【排序号】和【文件夹名称】文本框中分别输入“1”和“企业文化文件”，单击【确定】按钮。



图 13-105　【新建文件夹】页面

05 新文件夹创建成功，如图 13-106 所示，可以看到刚建立的公共文件夹，单击【企业文化文件】后面的【权限设置】链接。



图 13-106　新文件夹创建成功

06 打开权限设置页面，默认权限设置为【访问权限】，如图 13-107 所示，单击【授权范围

（人员）】文本框后面的【添加】按钮。

07 弹出【选择人员】对话框，选择具有权限访问“企业文化文件”公共文件柜的员工。本实例中要求所有员工都有权利访问，如图 13-108 所示，选中【郑州分公司】复选框，单击【确定】按钮。



图 13-107　权限设置页面

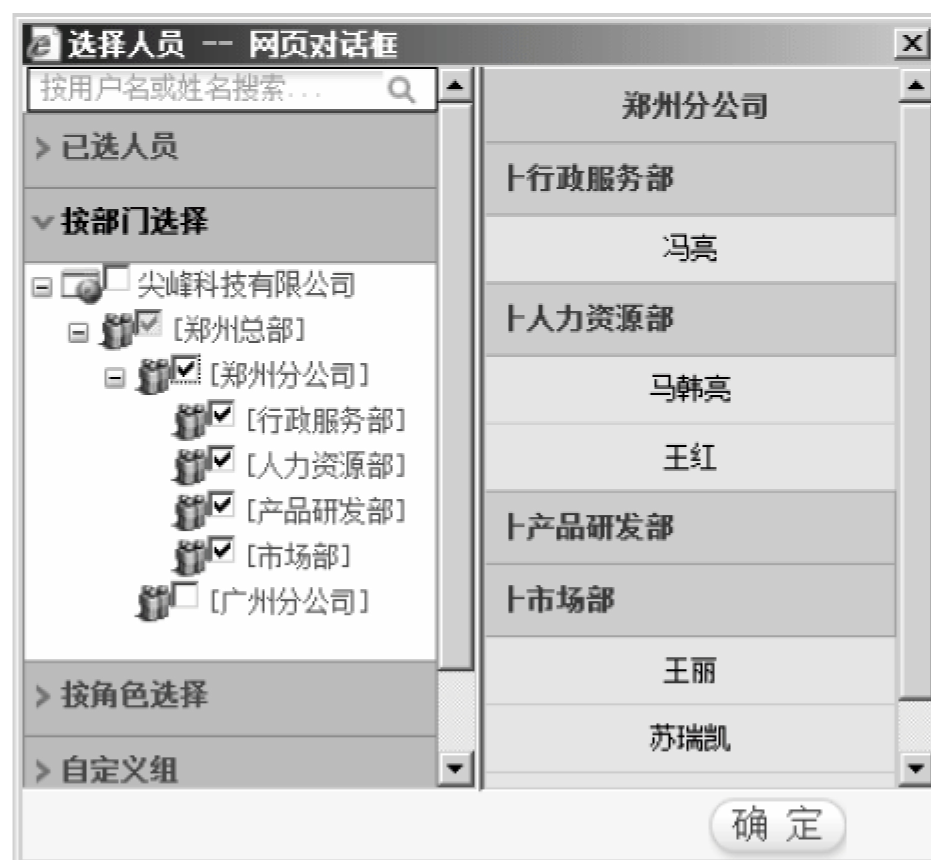


图 13-108　【选择人员】对话框

08 返回至权限设置页面，单击【确定】按钮。

09 权限设置完成，如图 13-109 所示，单击【新建权限】标签。



图 13-109　权限设置完成

10 如图 13-110 所示，单击【授权范围（人员）】文本框后面的【添加】按钮。

11 弹出【选择人员】页面，选择具有权限在“企业文化文件”公共文件柜中新建文件或文件夹的员工。本实例中要求郑州分公司人力资源部经理马韩亮有此权利，选择人力资源经理【马韩亮】，单击【确定】按钮。



图 13-110 【新建权限】页面

12 返回至【新建权限】页面，单击【确定】按钮。

13 返回至权限设置页面，单击【删除权限】标签，如图 13-111 所示，单击【授权范围（人员）】后面的【添加】按钮。



图 13-111 【删除权限】页面

14 弹出【选择人员】对话框，选择具有权限在“企业文化文件”目录中删除文件或文件夹的人员，本实例要求郑州分公司人力资源部经理马韩亮有此权利，选择【马韩亮】，单击【确定】按钮。

15 返回至权限设置页面，单击【确定】按钮。

16 返回至权限设置页面，单击【下载/打印权限】标签，单击【授权范围（人员）】文本框后面的【添加】按钮。

17 弹出【选择人员】对话框，选择拥有权利在“企业文化文件”文件夹中下载资源的员工，本实例要求所有员工都有权利下载资源，选中【郑州分公司】复选框，单击【确定】按钮。

18 返回至权限设置页面，单击【确定】按钮。

19 弹出【权限设置完成】提示框，表示权限设置完成。

20 使用郑州分公司人力资源经理“马韩亮”的账号进行登录 OA 系统。

21 弹出马韩亮的 OA【个人桌面】操作界面，如图 13-112 所示，选择【菜单】➢【知识管理】➢【公共文件柜】命令。



图 13-112 【个人桌面】操作界面

22 打开【公共文件柜】页面，如图 13-113 所示，单击左侧【企业文化文件】图标。



图 13-113 【公共文件柜】页面

23 如图 13-114 所示，单击【新建文件】按钮。



图 13-114 【公共文件柜】页面

24 打开【新建文件】页面，如图 13-115 所示，在【文件名称】和【排序号】文本框中分别输入相关内容，选中【Word 文档】单选按钮，单击【附件选择】一行后面的【添加附件】按钮。

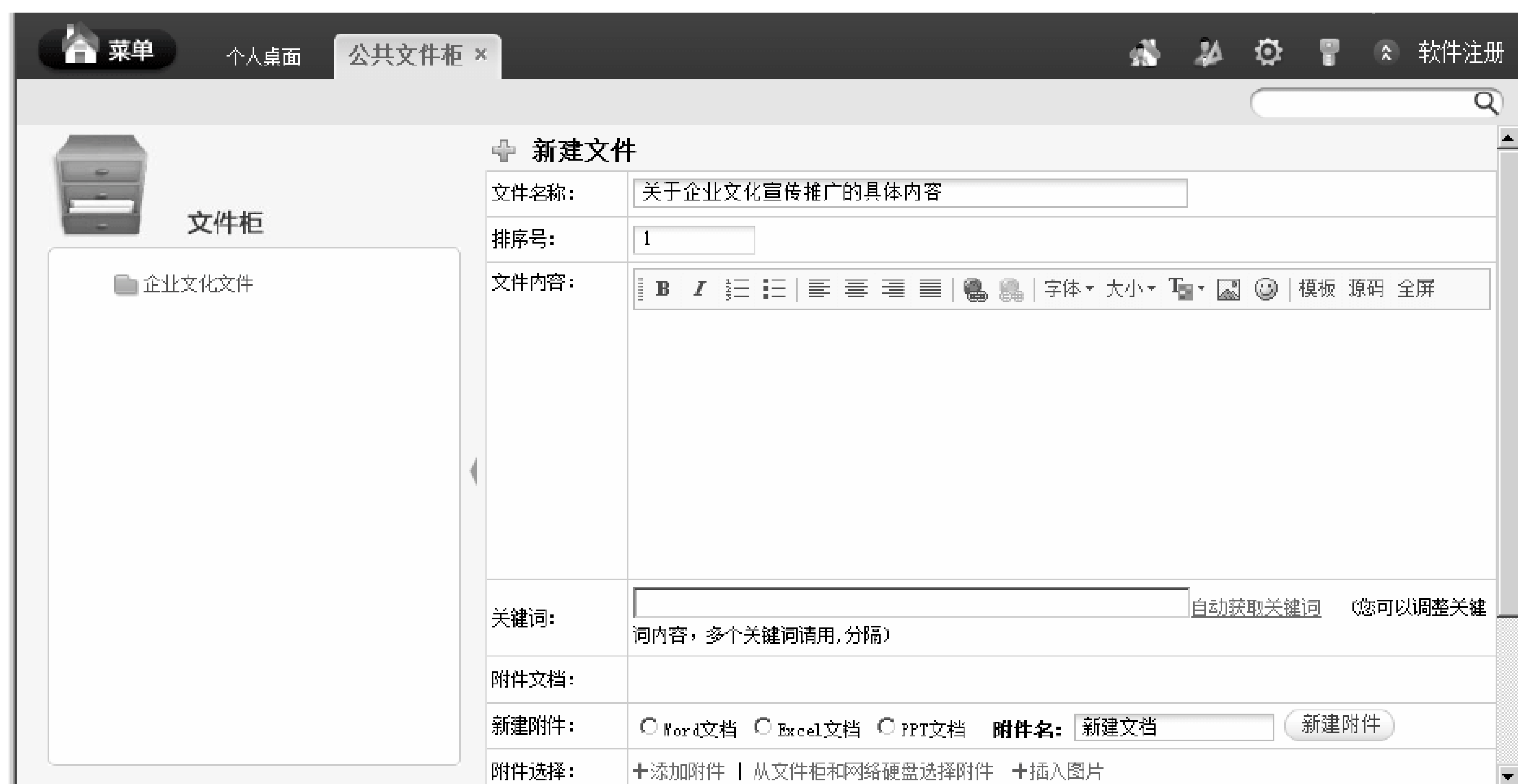


图 13-115 【新建文件】页面

25 弹出【选择要加载的文件】对话框，找到要上传的文件，如图 13-116 所示，单击【打开】按钮。



图 13-116 【选择要加载的文件】对话框

26 返回至【新建文件】页面，如图 13-117 所示，单击【上传附件】链接。



图 13-117 【新建文件】页面

27 如图 13-118 所示，单击【确定】按钮。



图 13-118 【新建文件】页面

28 返回至【公共文件柜】页面，如图 13-119 所示，如果需要下载该资源，选中【关于企业文化宣传推广的具体内容】复选框，单击【下载】按钮。



图 13-119 【公共文件柜】页面

29 弹出【文件下载】提示框，如图 13-120 所示，单击【保存】按钮。

30 弹出【另存为】对话框，找到该文件存储位置，如图 13-121 所示，单击【保存】按钮，完成下载。

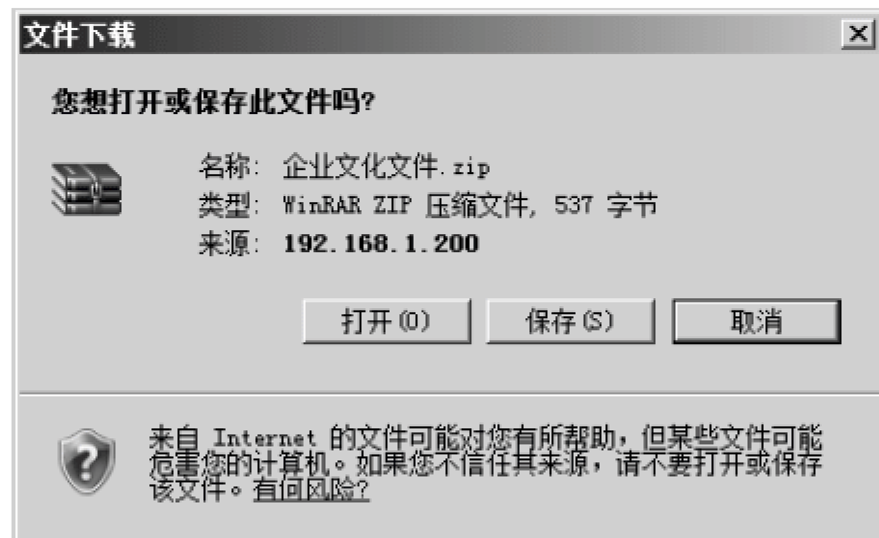


图 13-120 【文件下载】提示框

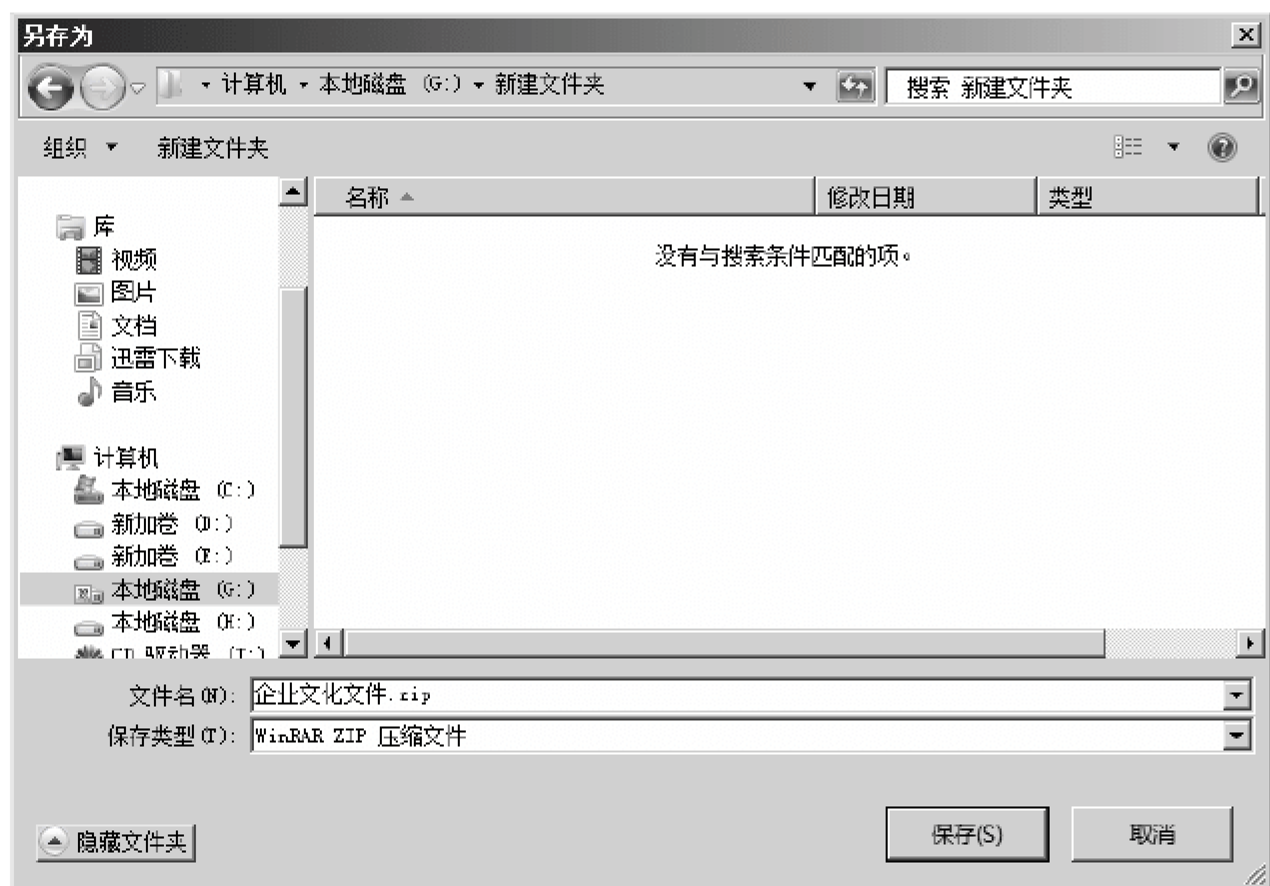


图 13-121 【另存为】对话框

13.4 企业工作流的创建与使用

13.4.1 工作流概述

在企业中为了完成某一项工作，总是需要经历很多的流程。例如请假，需要首先提出申请，然后再由各级领导审批，审批通过后还要交由人事部门登记备案。这种流程就是工作流。

依靠传统方式实现工作流会受到各部门人员时间的影响，例如当申请人提出请假申请时，某一个领导可能出差或在开会，当领导有时间时，申请人有可能已经下班或者有其他事情要忙。这样会严重影响工作流的效率。使用通达 OA2010 工作流功能可以非常轻松地实现各种类型的工作流，各级领导使用个人的 OA 账户就可以独立完成工作流的各个环节操作，可以大大提高工作效率。

13.4.2 项目实战 3：创建企业出差请假工作流

01 打开 IE 浏览器，在地址栏里面输入“http://192.168.1.200”，按 Enter 键，打开通达 OA2010 登录界面，在【用户名】对话框中输入“admin”，管理员的默认密码为空，单击【登录】按钮。

02 弹出管理员 OA【个人桌面】操作界面，如图 13-122 所示，选择【菜单】➢【系统管理】➢【工作流设置】➢【设计表单】命令。



图 13-122　【设计表单】选项

03 打开【设计表单】页面，如图 13-123 所示，在【表单名称】文本框中输入表单名称“出差申请单”，单击【保存】按钮。



图 13-123　【设计表单】页面

04 打开【表单管理】页面，如图 13-124 所示，单击【出差申请单】后面的【智能设计器】链接。



图 13-124　【表单管理】页面

05 弹出【表单智能设计器】界面，制作如图 13-125 所示的出差申请电子表单。将光标移动到【申请人】后面的单元格中，单击【单行输入框】按钮。

06 弹出【单行输入框属性】对话框，在【名称】文本框中输入名称为“申请人”，在【对齐方式】下拉列表框中选择【居中】，如图 13-126 所示，单击【确定】按钮。

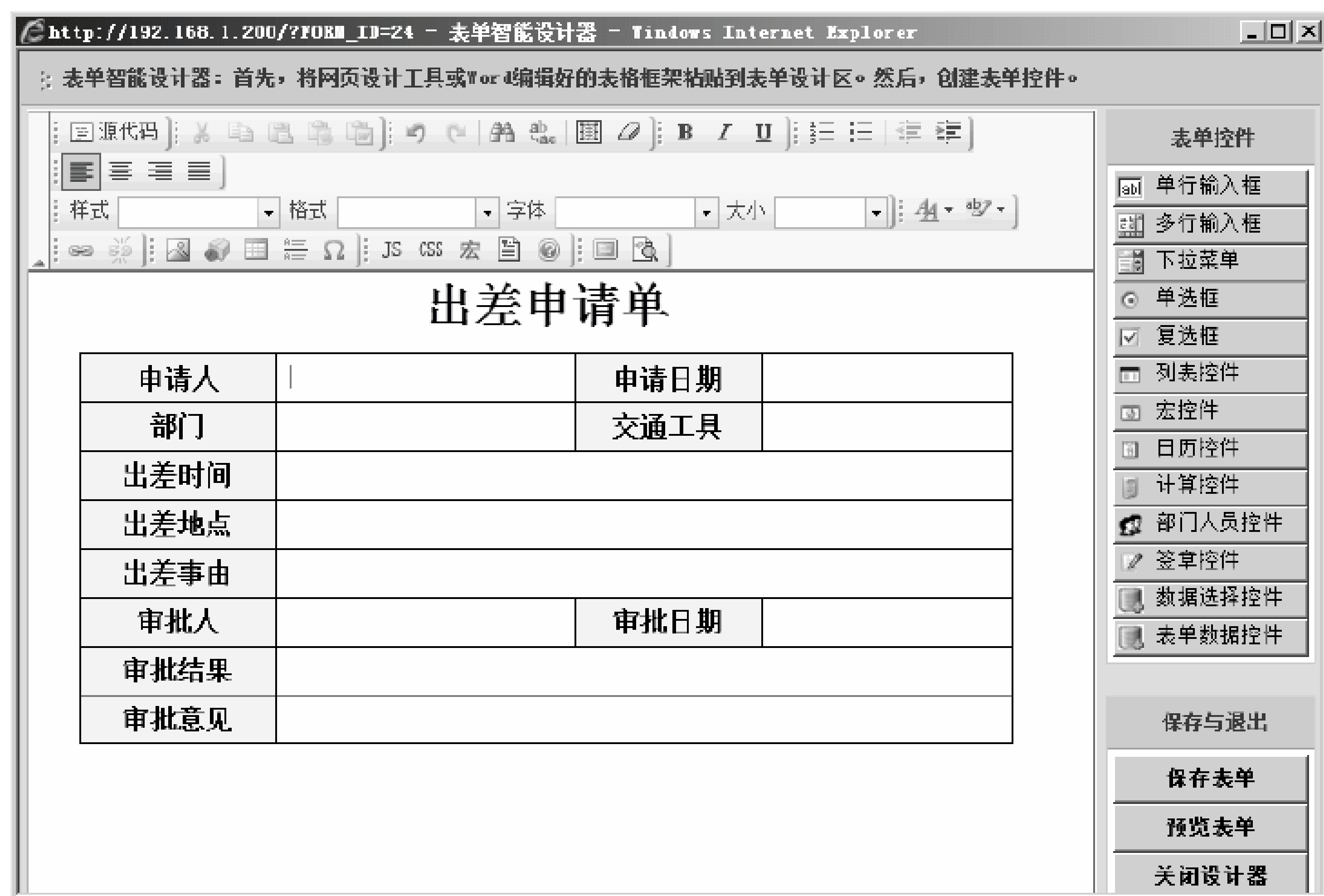


图 13-125 【表单智能设计器】界面

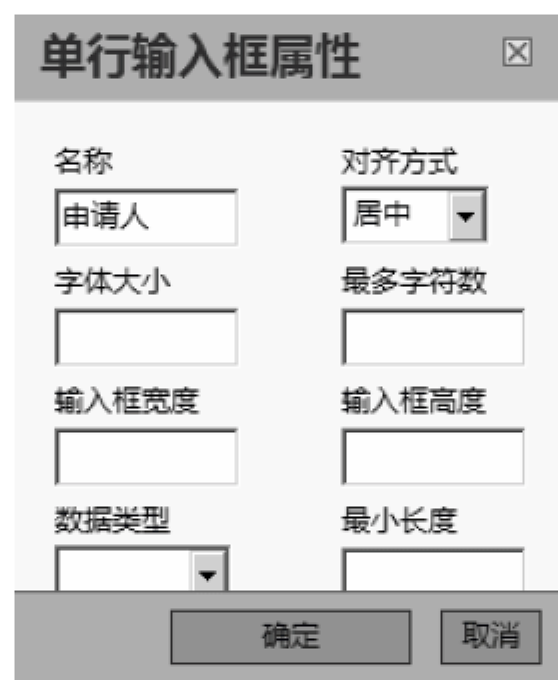


图 13-126 单行输入框属性

07 返回至【表单智能设计器】界面，如图 13-127 所示，将光标移动至【申请日期】后面的单元格中，单击【单行输入框】按钮。

08 弹出【单行输入框属性】对话框，如图 13-128 所示，在【名称】文本框中输入名称为“申请日期”，单击【确定】按钮。

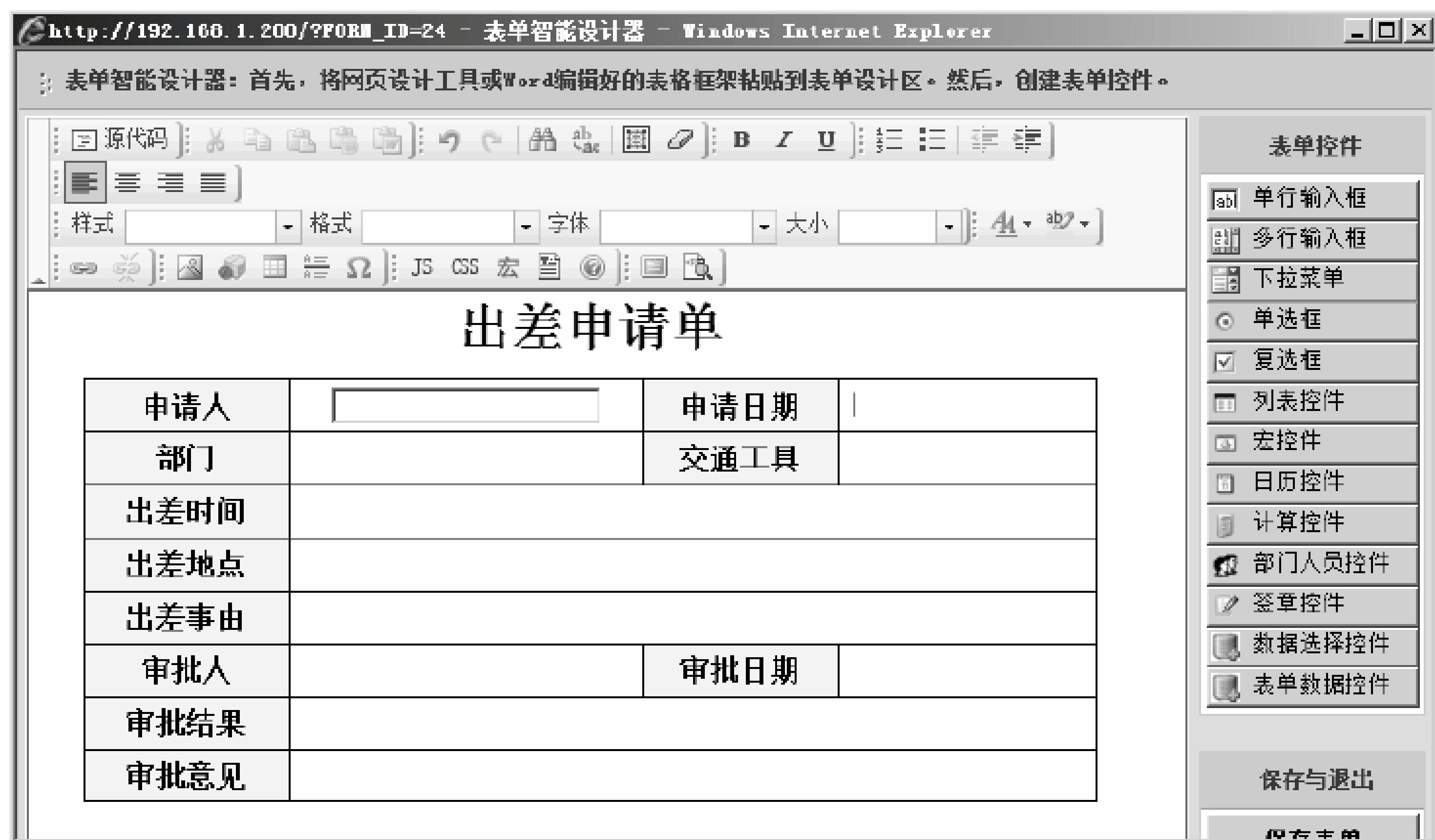


图 13-127 【表单智能设计器】界面

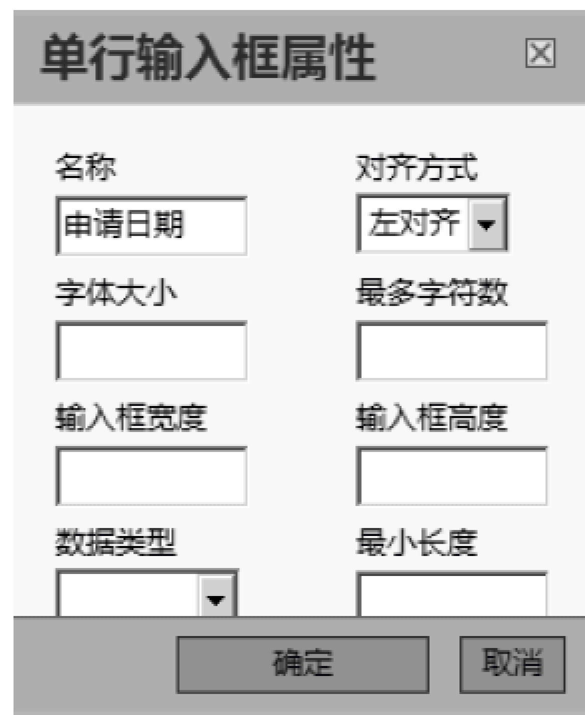


图 13-128 单行输入框属性

09 返回至【表单智能设计器】界面，如图 13-129 所示，单击【日历控件】按钮。

10 弹出【日历控件属性】对话框，在【输入框控件名称】文本框中输入名称为“申请日期”，注意这个地方的名称应该和上一控件名称一致，如图 13-130 所示，单击【确定】按钮。

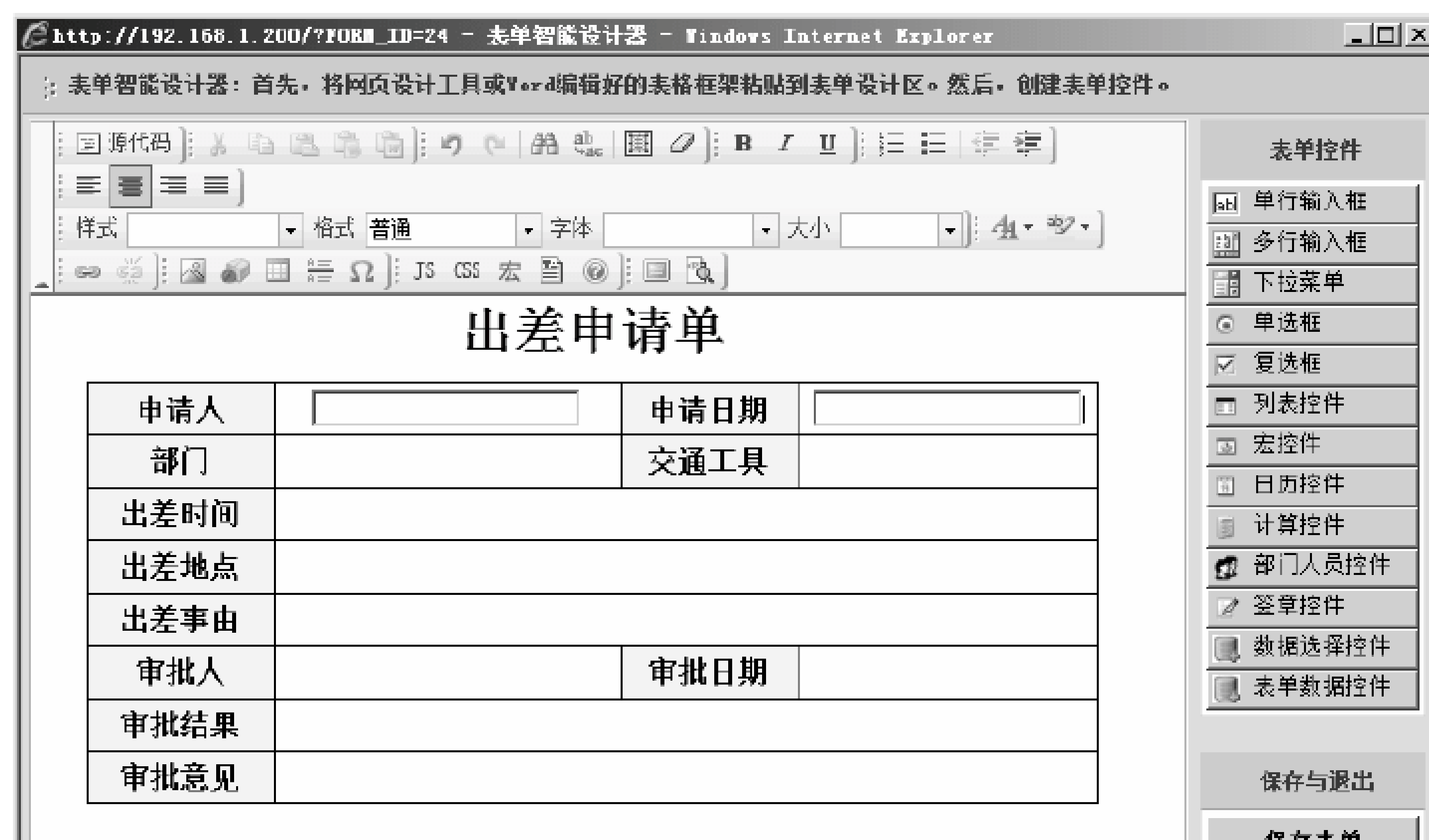


图 13-129　【表单智能设计器】界面

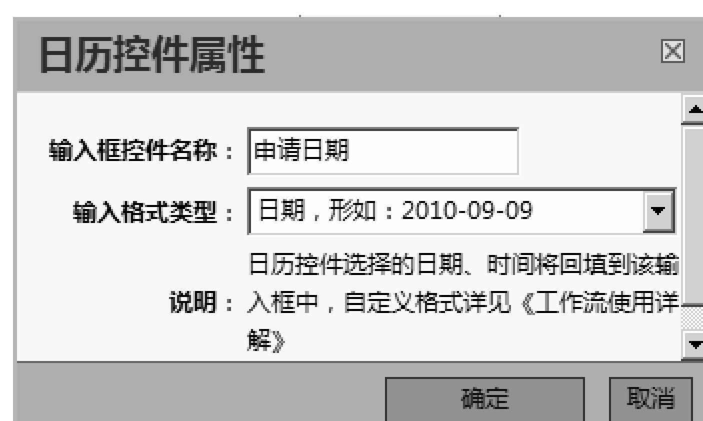


图 13-130　日历控件属性

11 返回至【表单智能设计器】界面，如图 13-131 所示，将光标移动至【部门】后面的单元格中，单击【单行输入框】按钮。

12 弹出【单行输入框属性】对话框，如图 13-132 所示，在【名称】文本框中输入名称为“部门”，单击【确定】按钮。

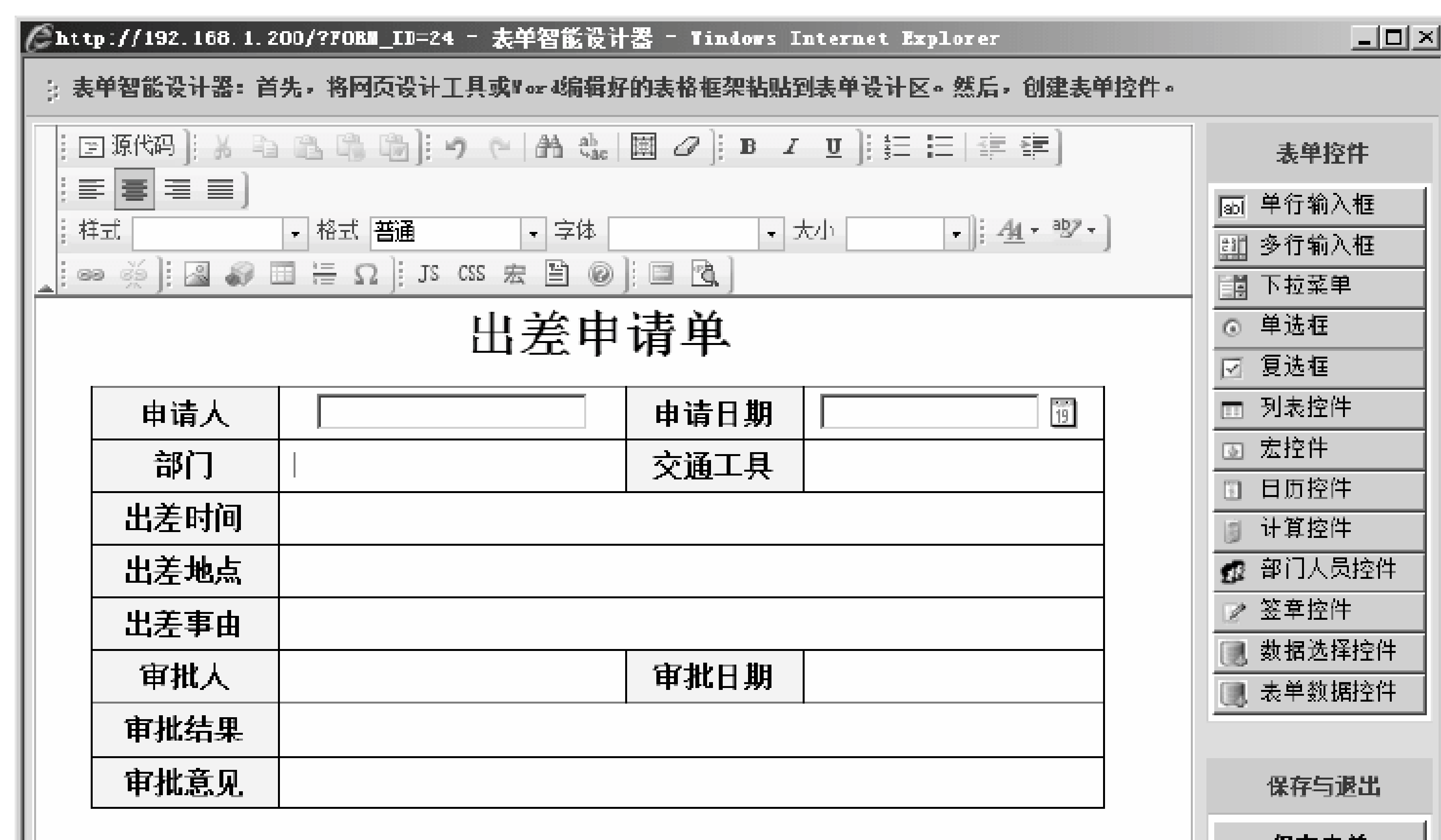


图 13-131　【表单智能设计器】界面

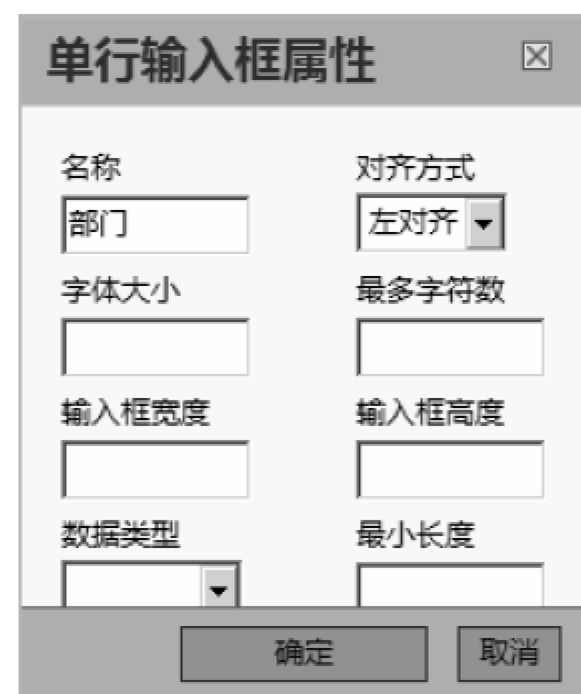


图 13-132　单行输入框属性

13 返回至【表单智能设计器】界面，如图 13-133 所示，单击【部门人员控件】按钮。

14 弹出【部门人员控件属性】对话框，在【对应的输入框控件名称】文本框中输入名称为“部门”，注意这个名称应该和上一控件名称一致。单击【选择类型】下拉菜单选择【选择部门】菜单命令，如图 13-134 所示，单击【确定】按钮。

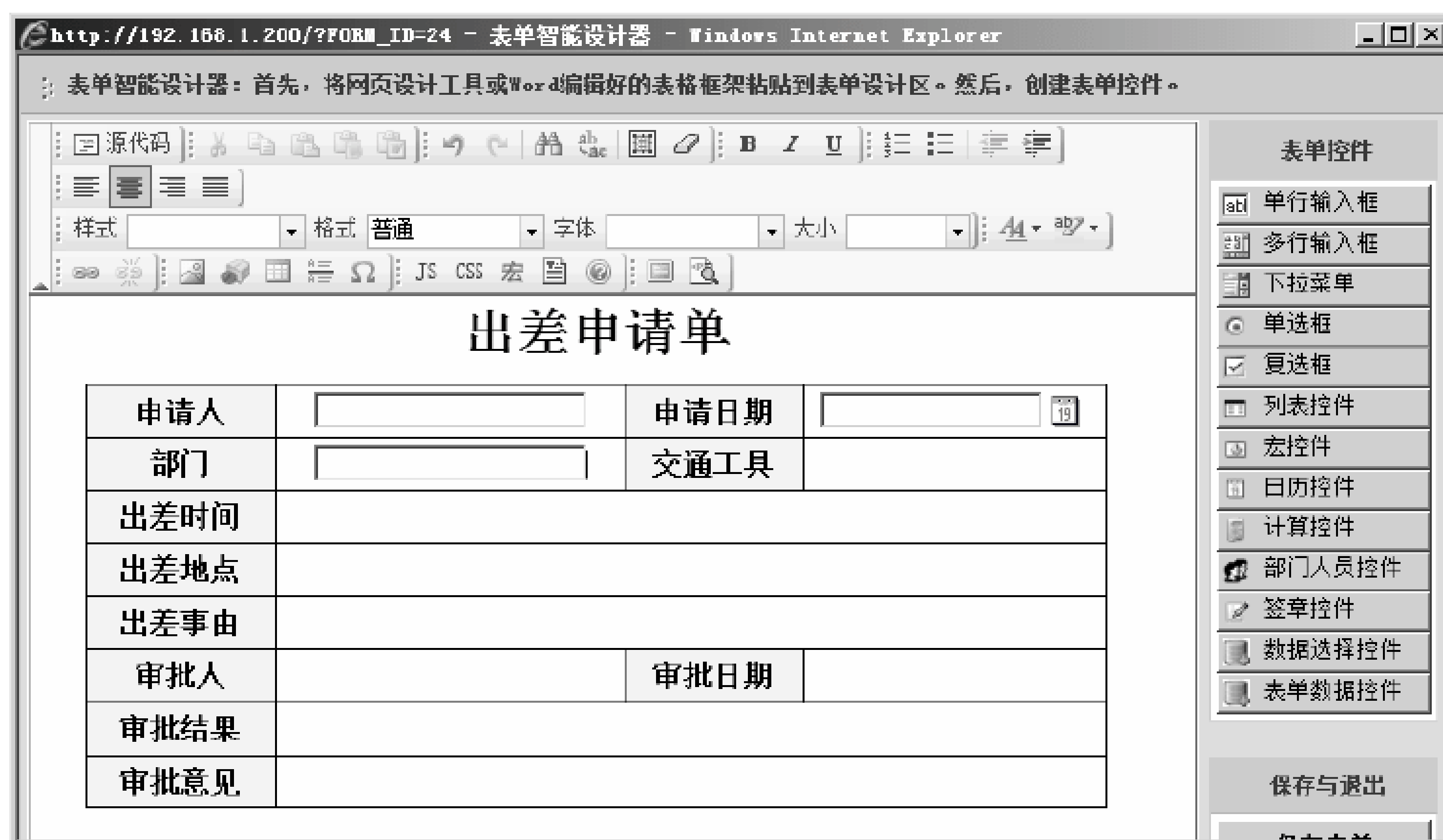


图 13-133 【表单智能设计器】界面

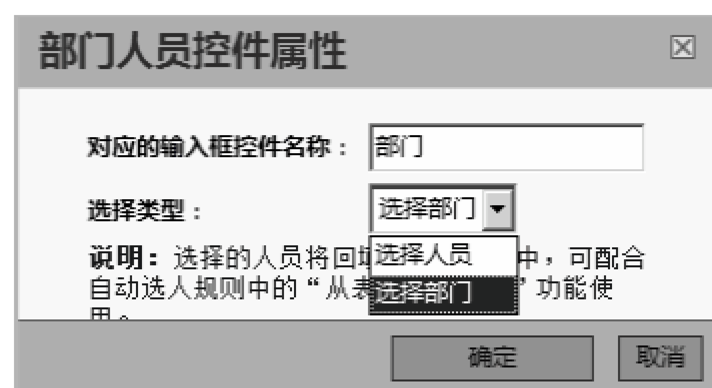


图 13-134 部门人员控件属性

15 返回至【表单智能设计器】界面，如图 13-135 所示，将光标移动至【交通工具】后面的单元格，单击【下拉菜单】按钮。

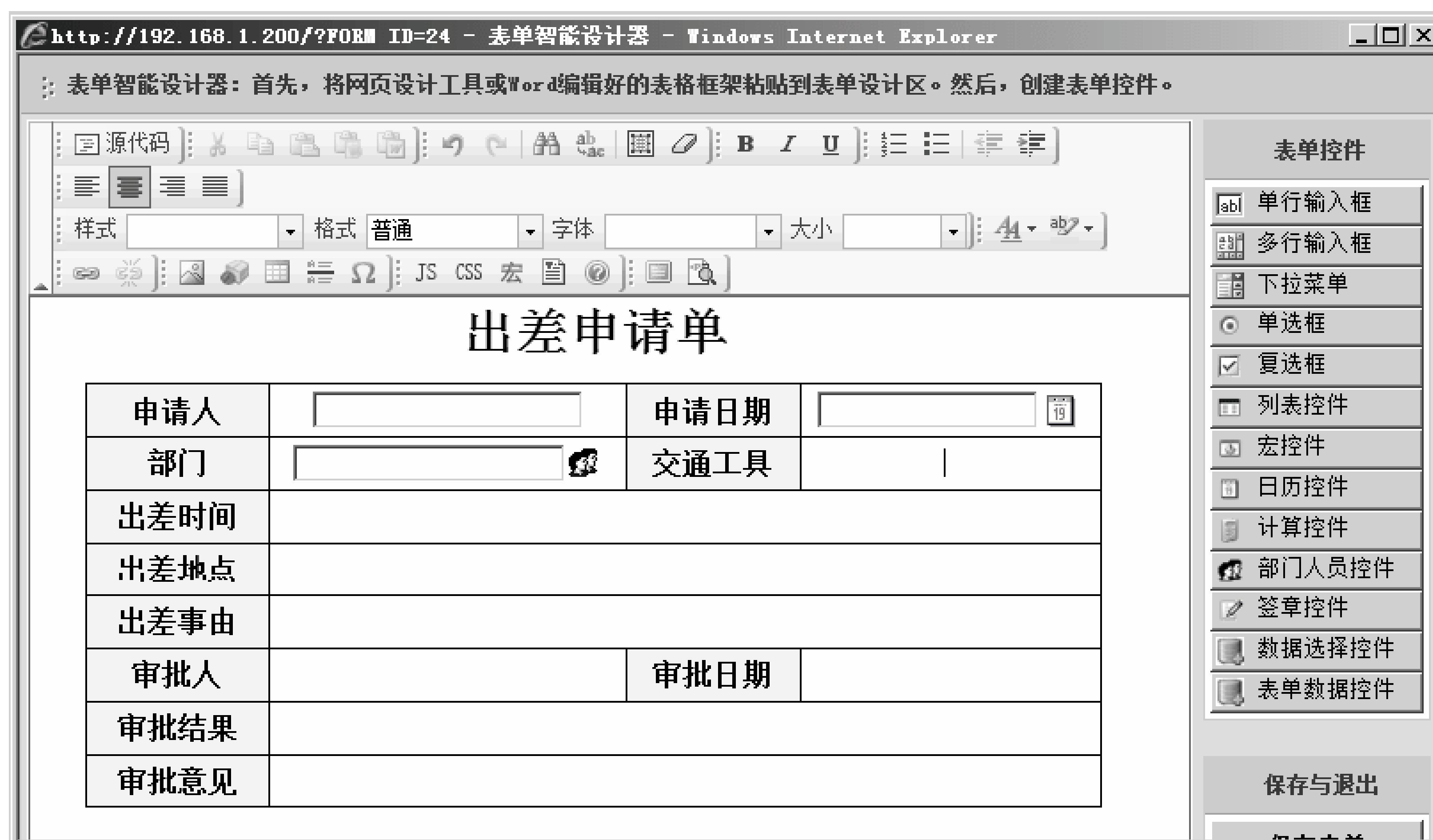


图 13-135 【表单智能设计器】界面

16 弹出【下拉菜单属性】对话框，在【控件名称】文本框中输入名称为“交通工具”，在【下拉菜单项目】文本框中输入“飞机”，单击【新增】按钮。如图 13-136 所示，依次添加“出租车”、“汽车”、“火车”等项目，单击【确定】按钮。



图 13-136　【下拉菜单属性】对话框

17 返回至【表单智能设计器】界面，如图 13-137 所示，将光标移动至【出差时间】后面的单元格中，单击【单行输入框】按钮。

18 弹出【单行输入框属性】对话框，在【名称】文本框中输入名称为“起始时间”，如图 13-138 所示，单击【确定】按钮。

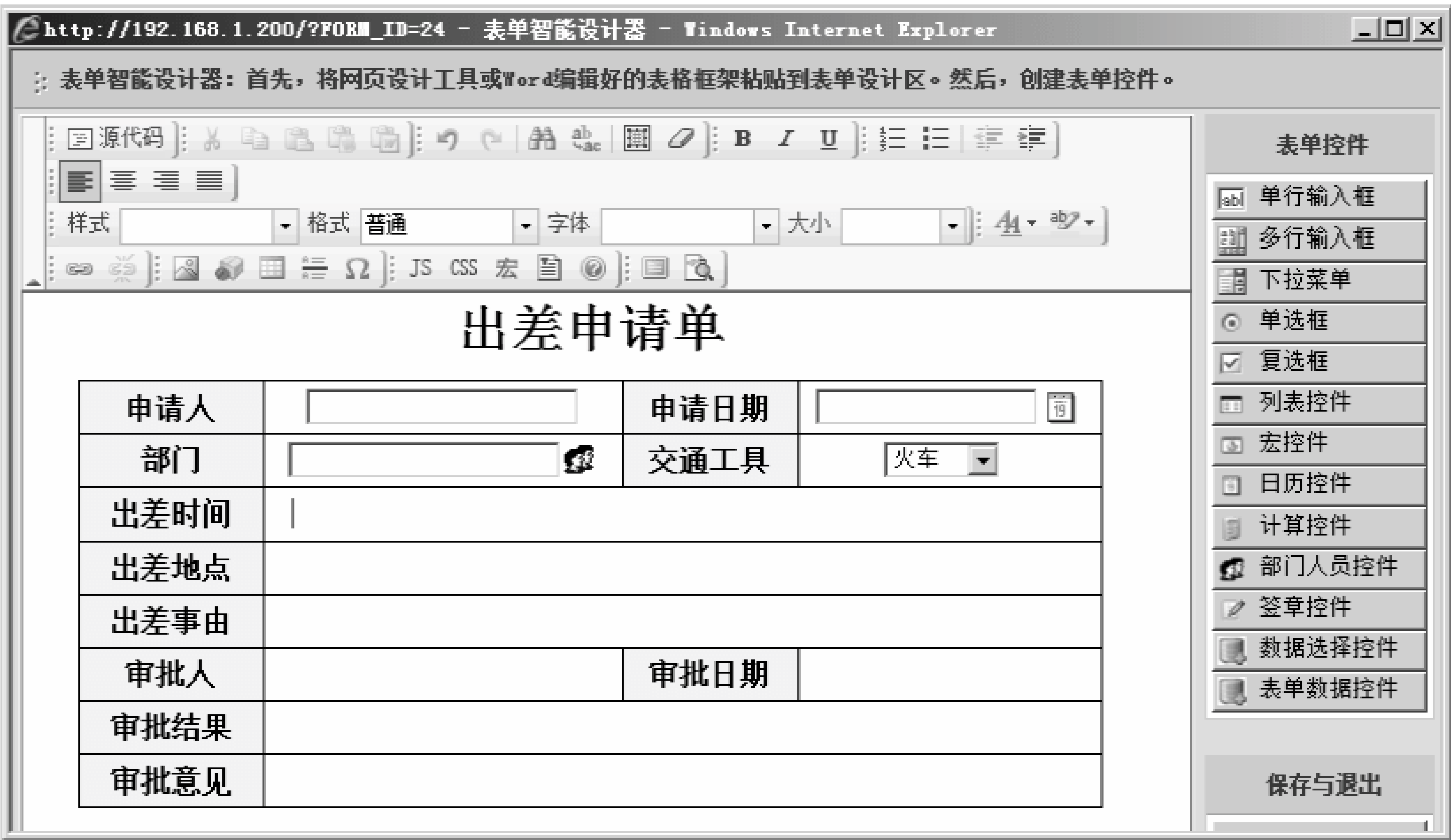


图 13-137　【表单智能设计器】界面

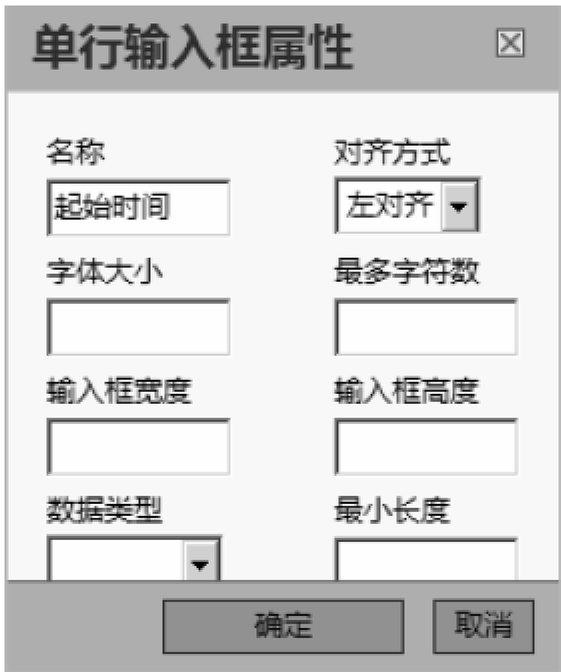


图 13-138　单行输入框属性

19 返回至【表单智能设计器】界面，如图 13-139 所示，单击【日历控件】按钮。

20 弹出【日历控件属性】对话框，如图 13-140 所示，在【输入框控件名称】文本框中输入名称为“起始时间”，单击【确定】按钮。

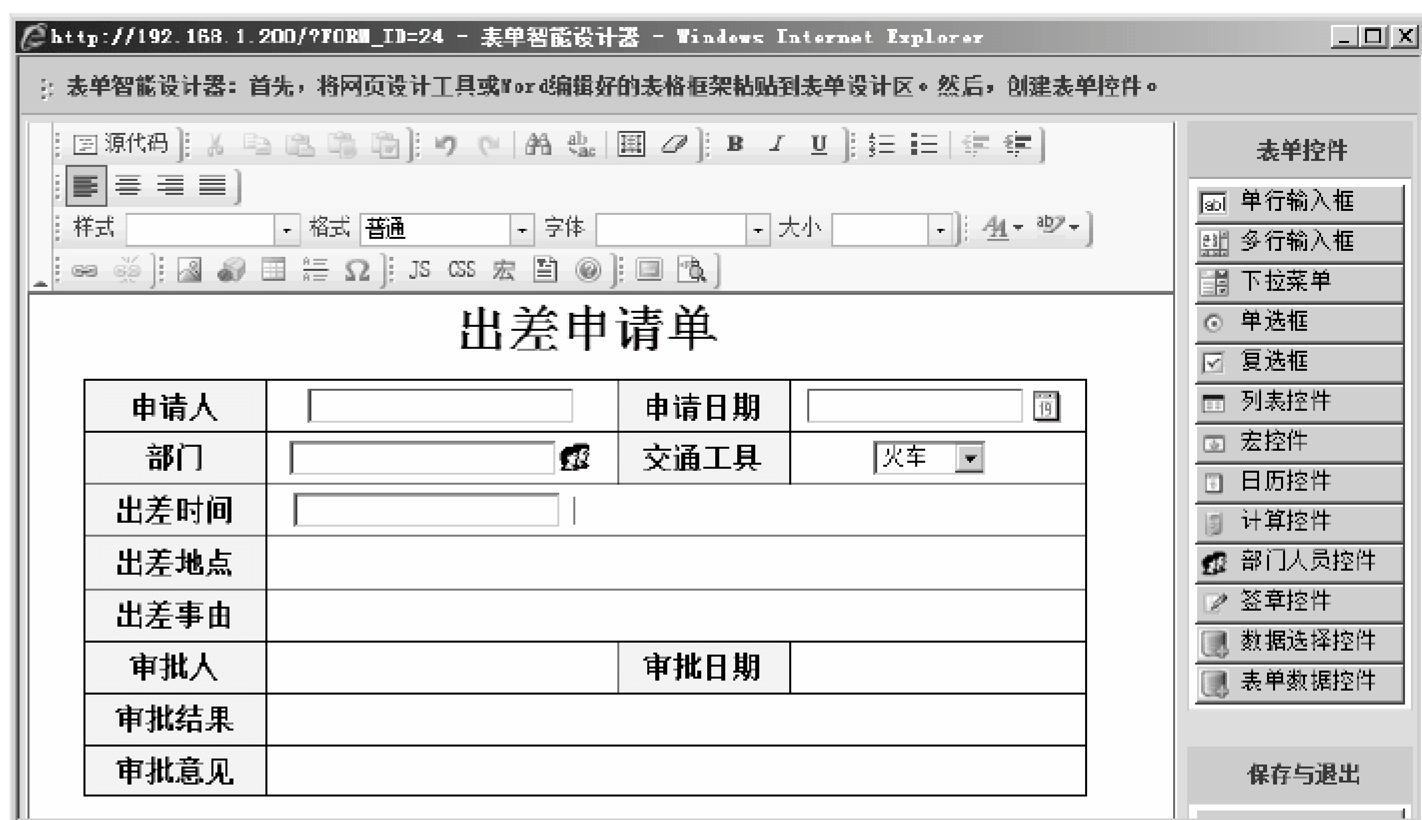


图 13-139 【表单智能设计器】界面

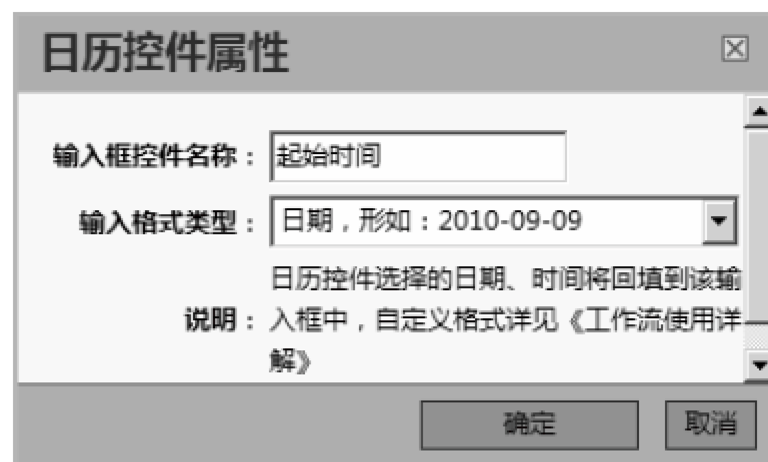


图 13-140 日历控件属性

21 返回至【表单智能设计器】界面，如图 13-141 所示，根据上一步骤添加【结束日期】文本框。



图 13-141 【表单智能设计器】界面

22 根据上述步骤，如图 13-142 所示依次完成【出差申请单】的各个控件添加，添加过程这里不再赘述，单击【保存表单】按钮。

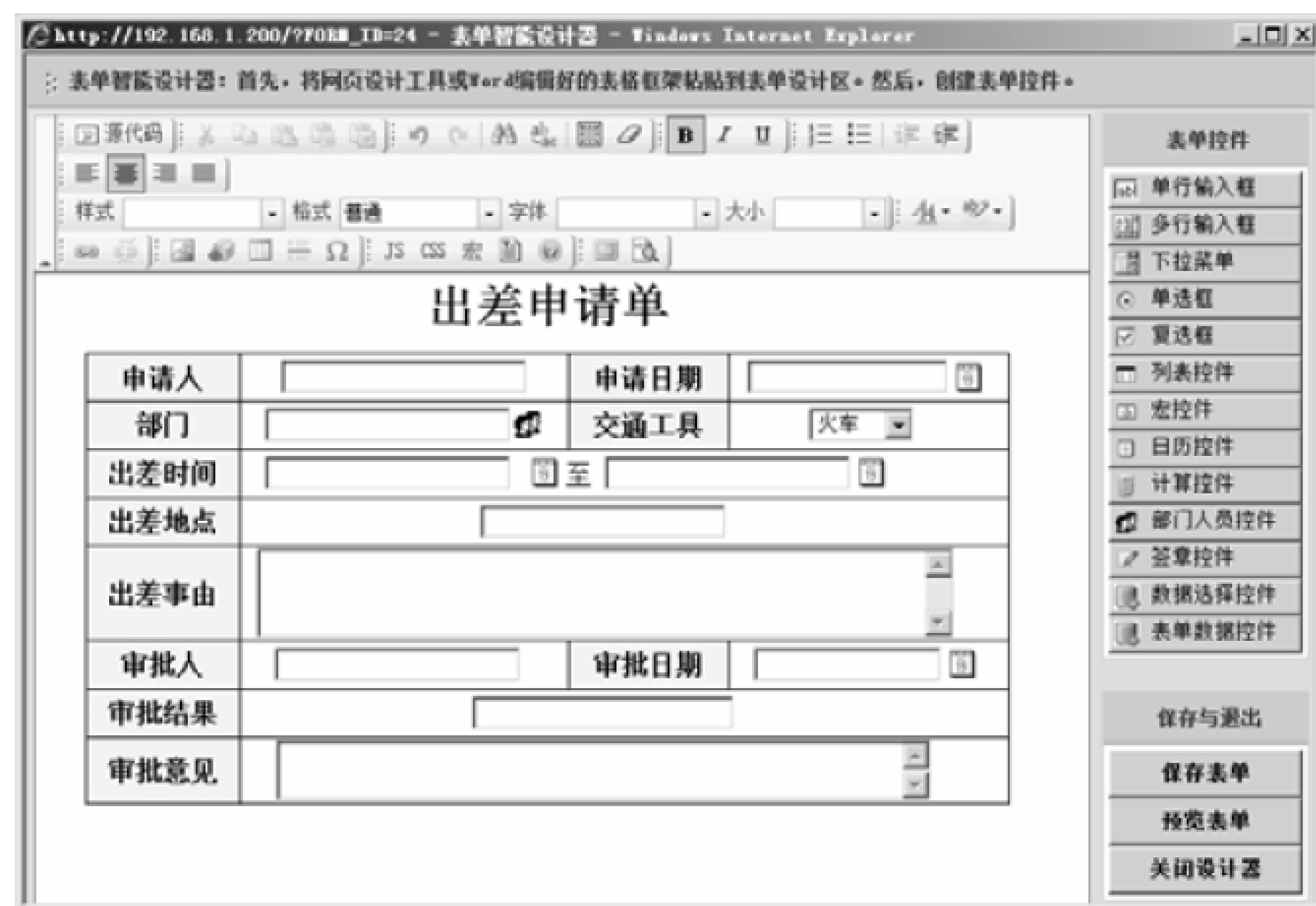


图 13-142 【表单智能设计器】界面

23 弹出【来自网页的消息】提示框，如图 13-143 所示，单击【确定】按钮。

24 返回至【设计表单】页面，选择【菜单】➢【系统管理】➢【工作流设置】➢【设计流程】命令。

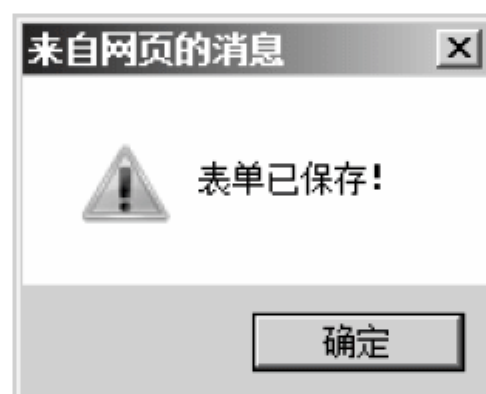


图 13-143 来自网页的消息

25 打开【设计流程】页面，如图 13-144 所示，在【流程分类】下拉列表框中选择【人事】，在【流程名称】文本框中输入名称为【出差申请流程】，在【所属部门】下拉列表框中选择【人力资源部】，单击【保存】按钮。



图 13-144 【设计流程】页面

26 返回至【设计流程】页面，如图 13-145 所示，单击【流程设计器】按钮。



图 13-145 【设计流程】页面

27 弹出【流程设计器】界面，如图 13-146 所示，单击【新建步骤】按钮。

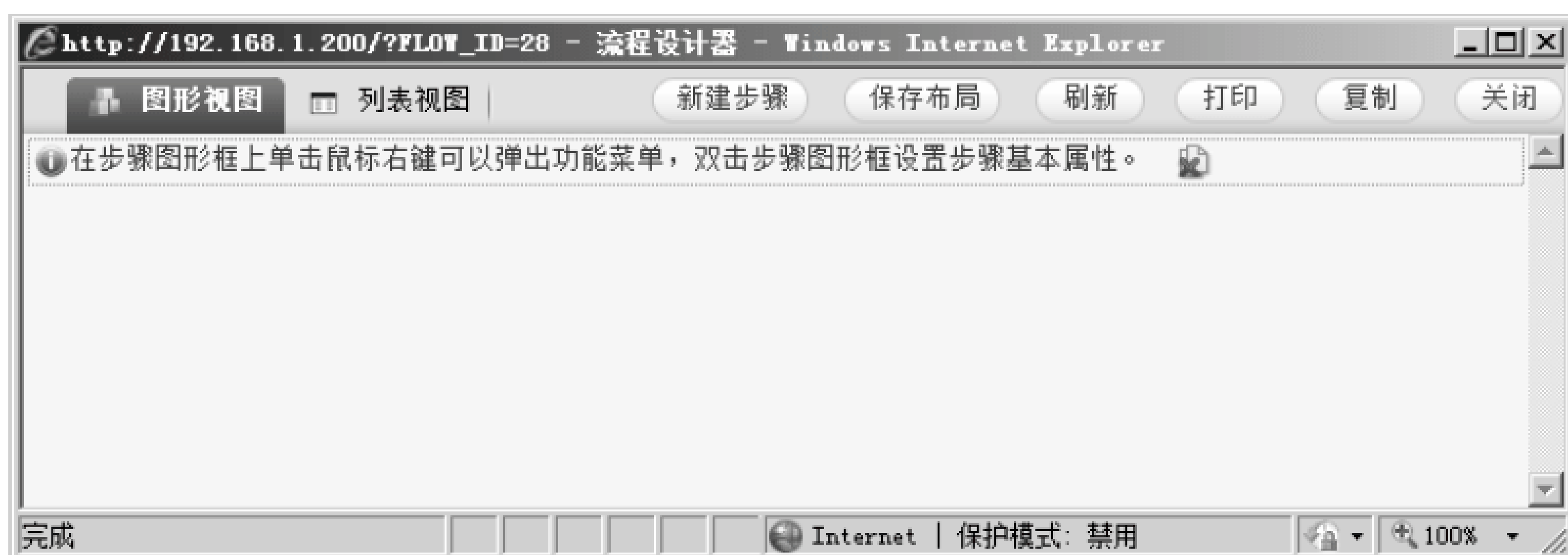


图 13-146 【流程设计器】界面

28 弹出【新建流程步骤】界面，如图 13-147 所示，在【序号】文本框中输入序号为 1，在【节点类型】下拉列表框中选择【步骤节点】，单击【保存】按钮。



图 13-147 【新建流程步骤】界面

29 弹出【系统提示】提示框，如图 13-148 所示，单击【设置】按钮。

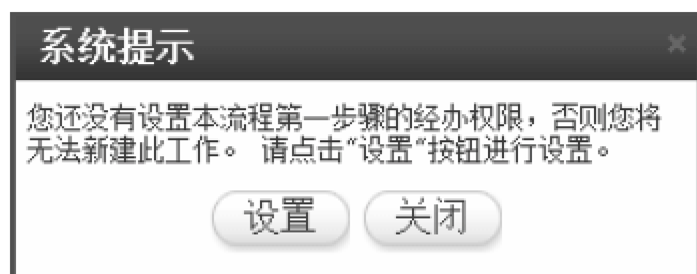


图 13-148 【系统提示】提示框

30 弹出【设置经办权限】界面，如图 13-149 所示，单击【授权范围（部门）】文本框后面的【添加】链接。

31 弹出【选择部门】对话框，选择具有权利经历该步骤的用户，本实例中所有员工都有可能出差，如图 13-150 所示，选中【郑州总部】复选框，单击【确定】按钮。



图 13-149　【设置经办权限】界面



图 13-150　【选择部门】对话框

32 返回至【设置经办权限】界面，如图 13-151 所示，单击【确定】按钮。



图 13-151　【设置经办权限】界面

33 返回至【流程设计器】界面，如图 13-152 所示，单击【新建步骤】按钮。

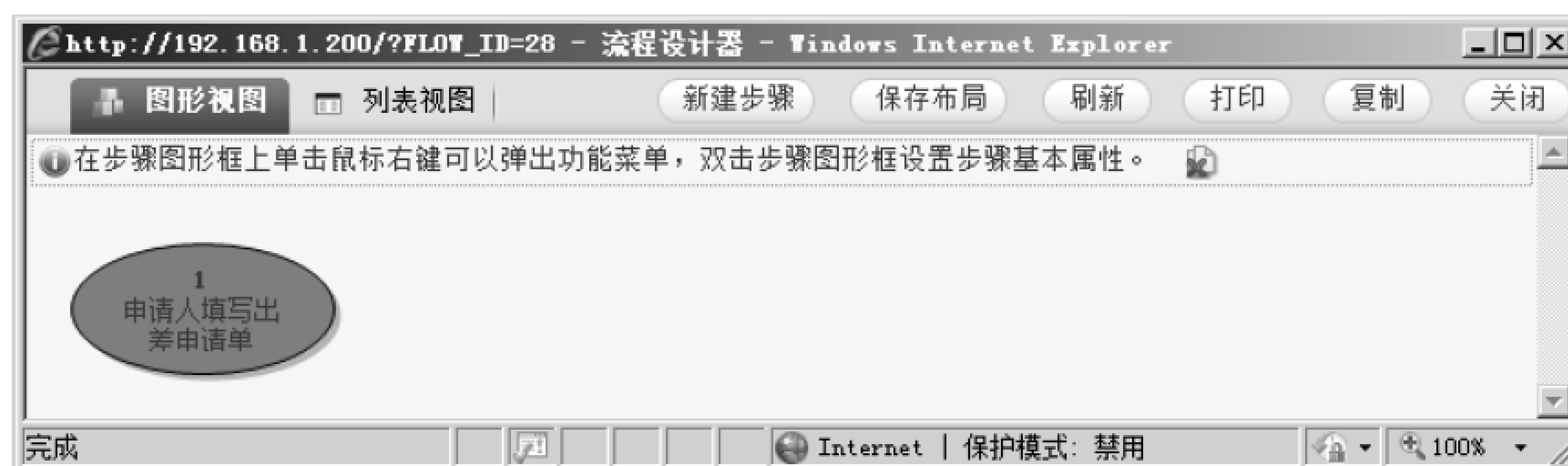


图 13-152　【流程设计器】界面

34 返回至【新建流程步骤】界面，如图 13-153 所示，在【序号】文本框后面输入序号为 2，

在【节点类型】下拉列表框中选择【步骤节点】，在【步骤名称】文本框中输入名称为“部门负责人审批”，单击【保存】按钮。



图 13-153 【新建流程步骤】界面

35 返回至【流程设计器】界面，如图 13-154 所示，单击【新建步骤】按钮。

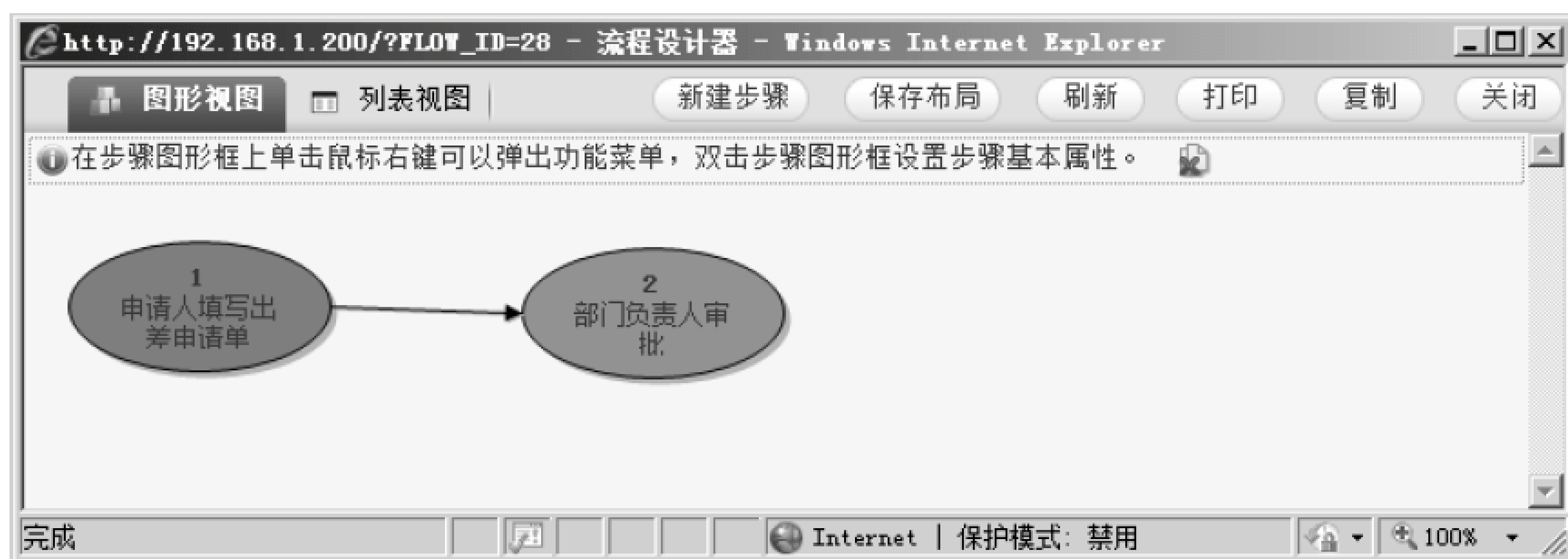


图 13-154 【流程设计器】界面

36 弹出【新建流程步骤】界面，如图 13-155 所示，在【序号】文本框后面输入序号为 3，在【节点类型】下拉列表框中选择【步骤节点】，在【步骤名称】文本框中输入名称为“人事部门备案”，单击【保存】按钮。



图 13-155　【新建流程步骤】窗口

37 返回至【流程设计器】窗口，如图 13-156 所示，右击步骤 1，在弹出的快捷菜单中选择【步骤基本属性】选项。

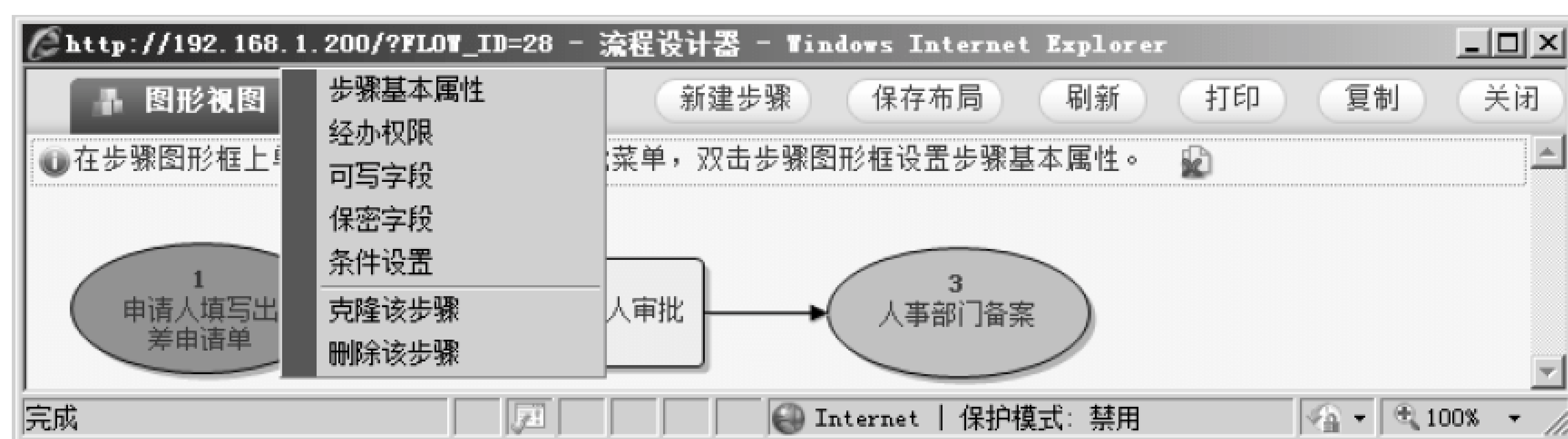


图 13-156　【流程设计器】界面

38 弹出【编辑流程步骤】界面，选择出差申请流程中第一个步骤的下一步骤。如图 13-157 所示，本实例中选择【备选步骤】列表框中的【部门负责人审批】选项，单击 ← 按钮，单击【保存】按钮。



图 13-157 【编辑流程步骤】界面

39 返回至【流程设计器】界面，右击步骤 1，在弹出的快捷菜单中选择【可写字段】命令。

40 弹出【编辑可写字段】界面，将出差申请流程中第一个步骤中申请人可以填写的字段添加为可写字段。选择【备选字段】中的【申请人】，然后单击 ← 按钮，将【申请人】字段添加为可写字段。如图 13-158 所示，依次添加【申请日期】、【部门】、【交通工具】、【起始时间】、【结束时间】、【出差地点】、【出差事由】等字段添加为可写字段，单击【保存】按钮。



图 13-158 【编辑可写字段】界面

41 返回至【流程设计器】界面，如图 13-159 所示，右击步骤 2，在弹出的快捷菜单中选择【步骤基本属性】选项。

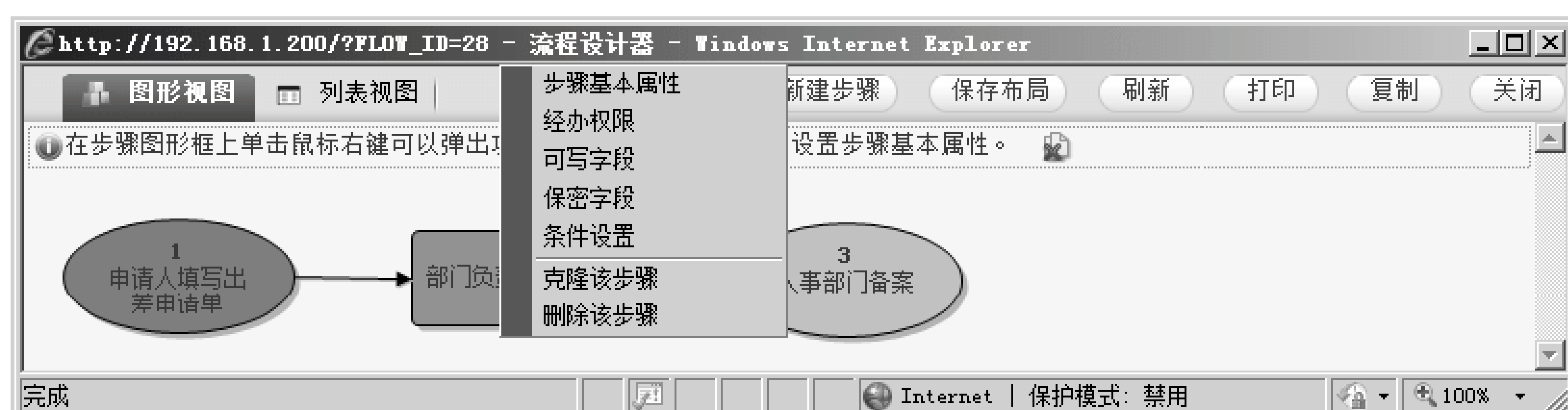


图 13-159　【流程设计器】界面

42 弹出【编辑流程步骤】界面，选择出差申请流程的第二个步骤的下一步骤。如图 13-160 所示，选择【备选步骤】列表框中的【人事部门备案】选项，单击 ← 按钮，然后单击【保存】按钮。



图 13-160　【编辑流程步骤】界面

43 返回至【流程设计器】界面，右击步骤 2，在弹出的快捷菜单中选择【经办权限】选项。

44 弹出【设置经办权限】界面，添加有权利经历该步骤的员工。本实例中只有经理有此权利，如图 13-161 所示，单击【授权范围（角色）】文本框后面的【添加】按钮。

45 弹出【选择角色】对话框，选择【部门经理】角色，单击【确定】按钮。



图 13-161　【选择角色】界面

46 返回至【设置经办权限】界面，如图 13-162 所示，单击【确定】按钮。



图 13-162 【设置经办权限】界面

47 返回至【流程设计器】界面，右击步骤 2，在弹出的快捷菜单中选择【可写字段】选项。

48 弹出【编辑可写字段】界面，将出差申请流程的第二个步骤中经办人可以填写的字段添加为可写字段。选择【备选字段】中的【审批人】，然后单击【←】按钮，将【审批人】字段添加为可写字段。如图 13-163 所示，依次添加【审批日期】、【审批结果】、【审批意见】等字段添加为可写字段，单击【保存】按钮。



图 13-163 【编辑可写字段】界面

49 返回至【流程设计器】界面，如图 13-164 所示，右击步骤 3，在弹出的快捷菜单中选择【步骤基本属性】选项。

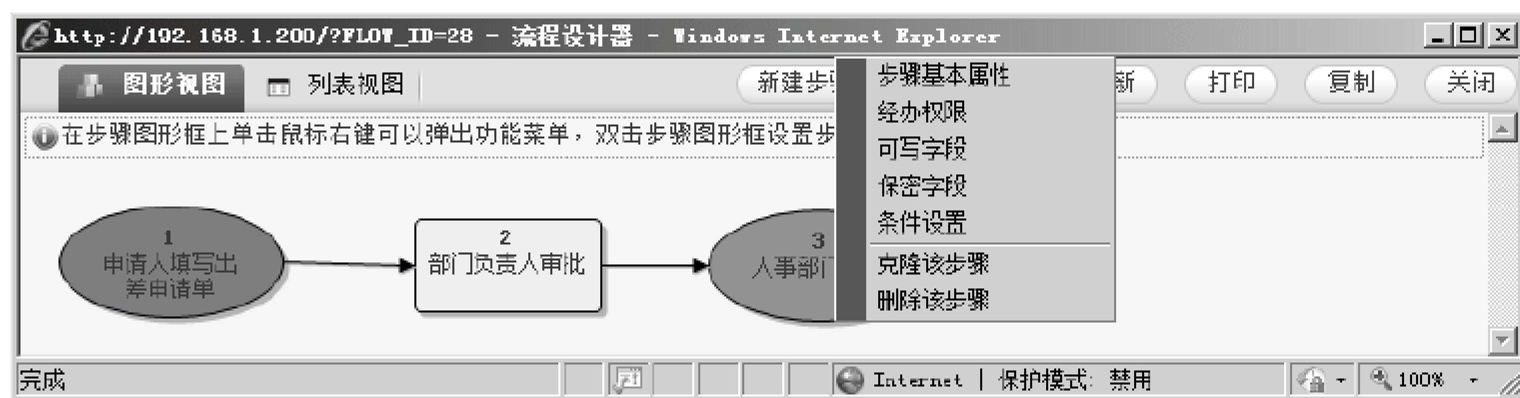


图 13-164　【流程设计器】界面

50 弹出【编辑流程步骤】界面，选择出差申请流程的第三个步骤的下一步骤。如图 13-165 所示，选择【备选步骤】列表框中的【结束流程】选项，单击 ← 按钮，单击【保存】按钮。



图 13-165　出【编辑流程步骤】界面

51 返回至【流程设计器】界面，右击步骤 3，在弹出的快捷菜单中选择【经办权限】选项。

52 弹出【设置经办权限】界面，如图 13-166 所示，单击【授权范围（角色）】文本框后面的【添加】按钮。

53 弹出【选择角色】对话框，选择【考勤专员】角色，单击【确定】按钮。



图 13-166 【设置经办权限】对话框

54 返回至【设置经办权限】界面，如图 13-167 所示，单击【确定】按钮。



图 13-167 【设置经办权限】界面

55 返回至【流程设计器】界面，单击【保存布局】按钮，保存流程后单击【关闭】按钮。

56 返回至【设计流程】界面，如图 13-168 所示，单击【保存】按钮，出差申请工作流建立完成。



图 13-168　【设计流程】界面

13.4.3　项目实战 4：出差请假工作流的实际使用

01 使用郑州分公司市场部员工“王晓涛”的账号进行登录 OA 系统，在【用户名】文本框中输入“wangxiaotao”，单击【登录】按钮。

02 弹出王晓涛的 OA【个人桌面】操作界面，如图 13-169 所示，选择【菜单】➢【工作流】➢【新建工作】命令。



图 13-169　【个人桌面】操作界面

03 打开【新建工作】页面，如图 13-170 所示，在左侧选择【人事】➢【出差申请流程】选项。



图 13-170　【新建工作】页面

04 打开【新建工作】页面，如图 13-171 所示，单击【新建并办理】按钮。



图 13-171 【新建工作】页面

05 弹出【出差申请单】界面，如图 13-172 所示，根据申请单要求如实填写内容，单击【转交下一步】按钮。

图 13-172 【出差申请单】界面

06 打开【转交下一步骤】页面，如图 13-173 所示，选中【部门负责人审批】复选框，单击【选择人员】按钮。

07 弹出【选择经办人和主办人】对话框，选择部门负责人，如图 13-174 所示，选中市场部经理【王丽】复选框，单击【确认】按钮。

图 13-173 【转交下一步骤】页面　　图 13-174 【选择经办人和主办人】对话框

08 返回至【转交下一步骤】页面，如图 13-175 所示，单击【确认转交】按钮，出差申请结

束，等待领导批复。

09 市场部经理王丽登录 OA 进行审批。在【用户名】文本框中输入市场部经理王丽的账户“wangli”，单击【登录】按钮。

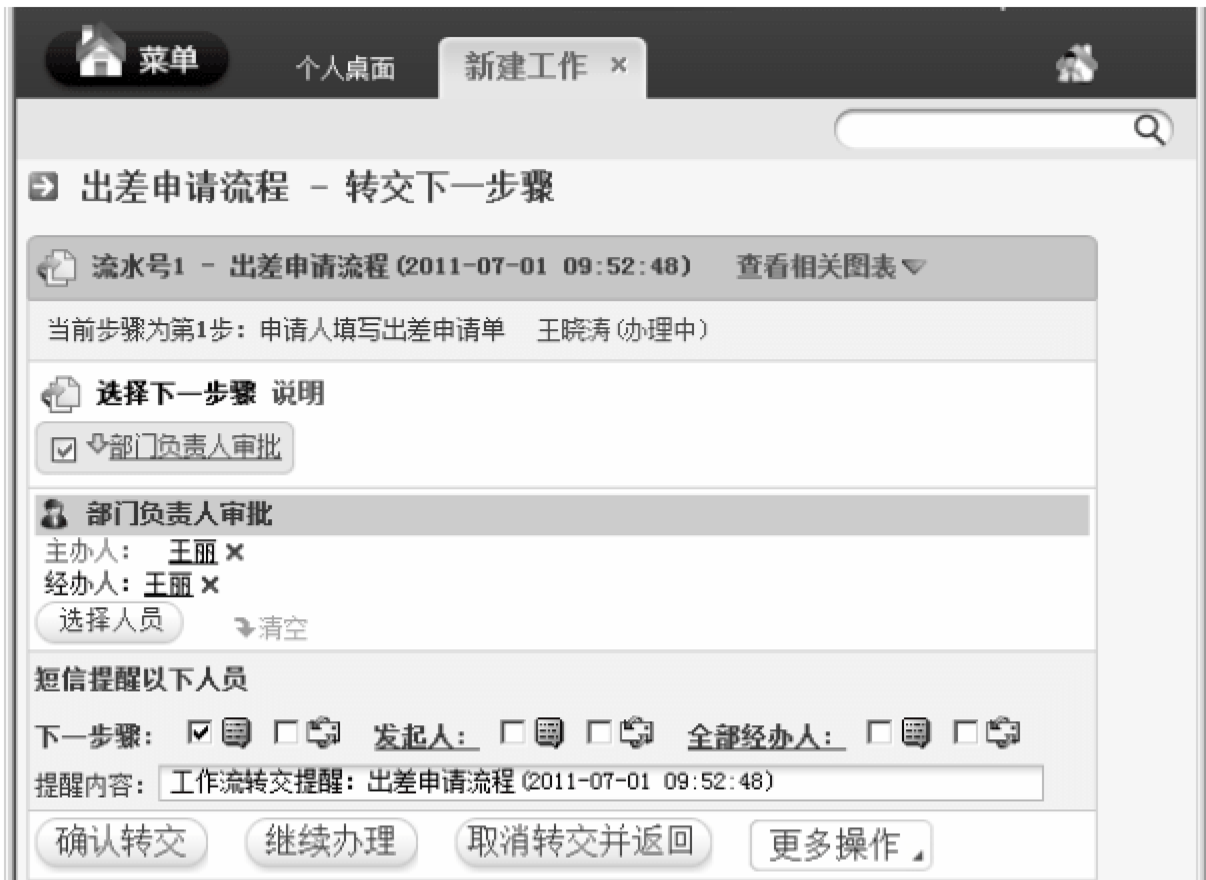


图 13-175　【转交下一步骤】页面

10 弹出王丽 OA【个人桌面】界面，如图 12-176 所示，单击【工作流】图标。



图 13-176　【个人桌面】界面

11 弹出【工作流】对话框，如图 12-177 所示，单击【出差申请流程】链接。



状态	流程类别	步骤名称	工作名称/文号
	出差申请流程	部门负责人审批	出差申请流程 (2011-07-01 09:52:48)

图 13-177　【工作流】对话框

12 弹出【我的工作】页面，在【审批人】、【审批日期】、【审批结果】和【审批意见】文本框输入相关信息，如图 13-178 所示，单击【转交下一步】按钮。

图 13-178 【我的工作】页面

13 打开【转交下一步骤】页面，如图 13-179 所示，单击【选择人员】按钮。

14 弹出【选择经办人和主办人】对话框，如图 13-180 所示，选中【王红】复选框，单击【确认】按钮。

图 13-179 【转交下一步骤】页面　　图 13-180 【选择经办人和主办人】对话框

15 返回至【转交下一步骤】页面，如图 13-181 所示，单击【确认转交】按钮，市场部经理王丽完成审批。

16 人事部考勤专员王红登录 OA 进行考勤备案。在【用户名】文本框中输入人力资源部考勤专员王红的账户“wanghong”，单击【登录】按钮。



图 13-181 【转交下一步骤】页面

17 弹出王红 OA【个人桌面】操作界面，单击【工作流】图标。

18 弹出【工作流】对话框，如图 13-182 所示，单击【出差申请流程】链接。



图 13-182 【工作流】对话框

19 打开【我的工作】页面，如图 13-183 所示，单击【转交】按钮。



图 13-183 【我的工作】页面

20 打开【转交下一步骤】页面，如图 13-184 所示，选中【结束流程】复选框，选中【发起人】后面的图标，单击【结束流程】按钮。

21 弹出【来自网页的消息】提示框，确认是否要结束流程，如图 13-185 所示，单击【确定】按钮，至此人事部备案结束。

22 出差申请人王晓涛登录 OA 查看审批结果。在【用户名】文本框中输入市场部员工王晓涛的账户“wangxiaotao”，单击【登录】按钮。



图 13-184 【转交下一步骤】页面

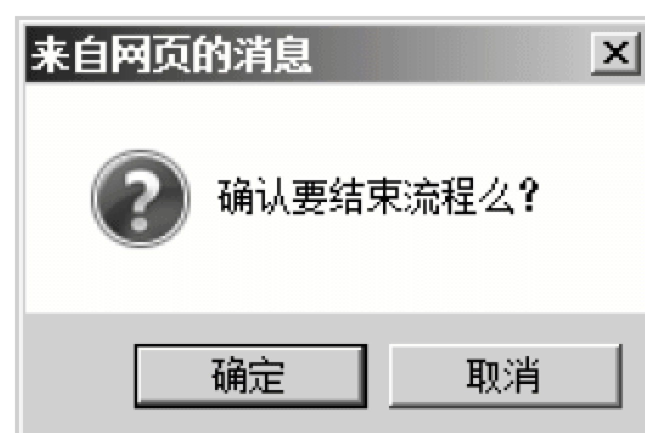


图 13-185 来自网页的消息

23 弹出王晓涛 OA【个人桌面】操作界面，单击【工作流】图标。

24 弹出【我的工作】页面，如图 13-186 所示，单击【已办结】图标，可以看到已经办理完的工作流，至此出差申请流程结束。



图 13-186 【我的工作】页面

13.5 专家答疑

（1）在创建工作流的时候为什么总是出现打不开【表单智能设计器】界面？

答：工作流是 OA 中最主要的应用，但是很多读者在设计工作流的时候，遇到【表单智能设计器】界面打不开的现象，这时候可以从两方面进行考虑，一方面是计算机的 IE 浏览器版本过低，另一方面是计算机的 IE 浏览器的安全级别设置得过高导致。

（2）OA 自动化系统在企业办公应用起到的作用越来越大，那么是不是建立了 OA 服务器后，对于企业的办公自动化就可以高枕无忧了呢？

答：正因为 OA 办公自动化在企业的核心应用使用得越来越多，网络管理人员更应该重视 OA 服务器。在架设完 OA 服务器后应该定期地对 OA 服务器进行维护，特别是对 OA 数据库进行定期备份。只有这样，OA 服务器出现意外事故的时候，才能及时恢复数据以保证企业的正常运行。

第 14 章　Windows 群集的管理

当前整个互联网信息交流访问量非常庞大，对于企业服务器来说，服务器必须能应付大量的请求信息。如果企业服务器面对的访问客户群体过大的话，只依靠单一的服务器很难应付。为了更好地提供互联网访问服务，群集技术诞生了。

Windows 服务器作为当前市场使用比较多的一种服务器平台环境，支持多种群集技术，如 NLB 群集、故障转移群集等。

14.1　Windows 群集概述

群集是使用多台服务器共同为客户机提供网络资源或服务的一种技术，在群集中每台服务器称为一个节点。使用群集技术可以提高网络服务的可用性和可靠性，当群集中的一台服务器故障时，其他服务器依然可以提供持续的网络资源或服务。

在 Windows Server 2008 中主要支持两种类型的群集：网络负载平衡群集和故障转移群集。

14.1.1　网络负载平衡群集

网络负载平衡（NLB）群集可以增强 Web、FTP、防火墙、代理和 VPN 等关键网络服务应用的可用性及可靠性。单靠一台服务器所能提供的服务性能毕竟有限，而使用网络负载平衡的群集技术，可以将多台服务器的性能整合在一起，共同提供服务，提高了服务的整体性能，这类似于人多力量大的道理。

在使用网络负载平衡群集时允许用户把两台或更多服务器结合起来使用，但是一个 NLB 群集最多支持 32 台服务器，而且 NLB 群集中各个服务器节点提供的服务和数据要完全相同。

图 14-1 所示为四个节点的 NLB 群集。

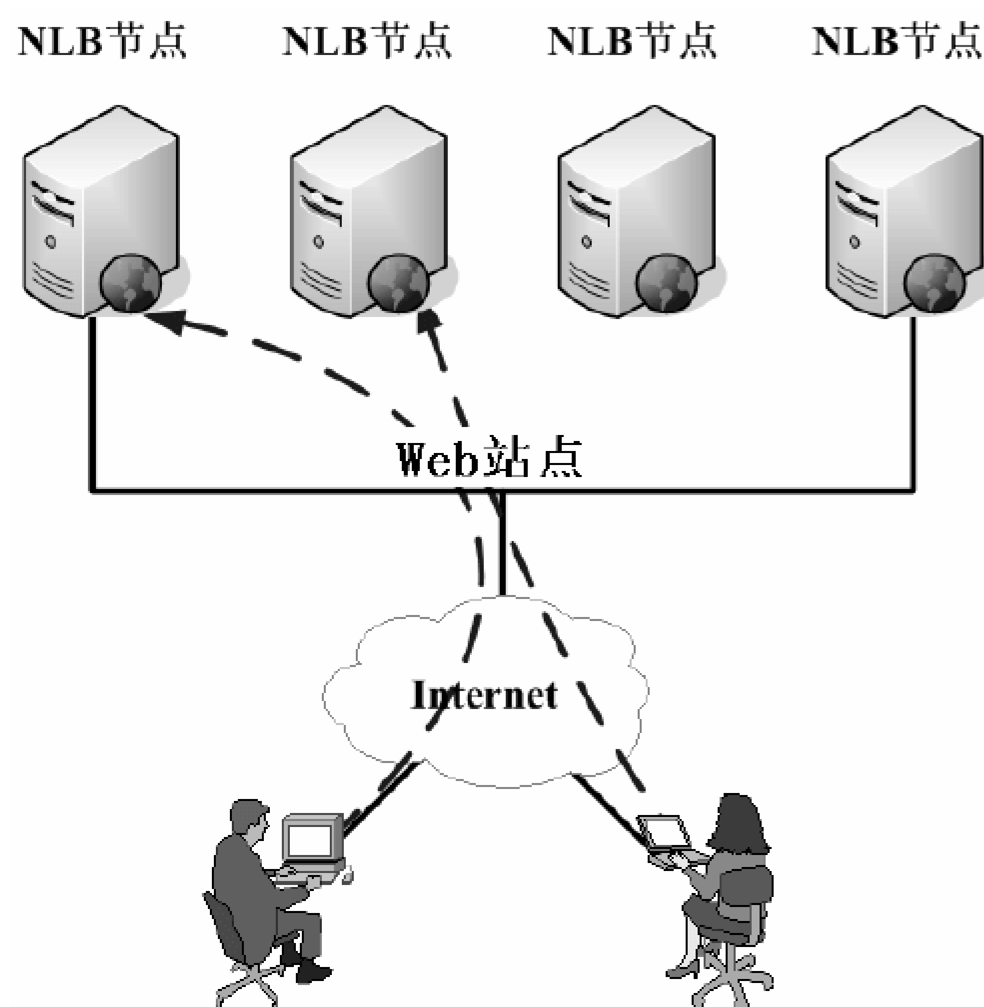


图 14-1　NLB 群集拓扑图

14.1.2　故障转移群集

故障转移群集是由独立的服务器系统构成的组，通过物理电缆和软件将各个节点连接起来协同工作，以达到增强应用程序和服务可靠性的目的。

其实故障转移群集的目的和 NLB 群集有些相似，但是故障转移群集的所有数据放在公共的存储设备上，该存储设备用于连接所有的群集节点，用于存储公共数据和仲裁数据。

在故障转移群集中，所有的节点并非平等的，有一个节点处于主动模式，其余节点处于被动模式，处于主动模式的节点可以建立、管理群集。

图 14-2 所示为双节点的故障转移群集。

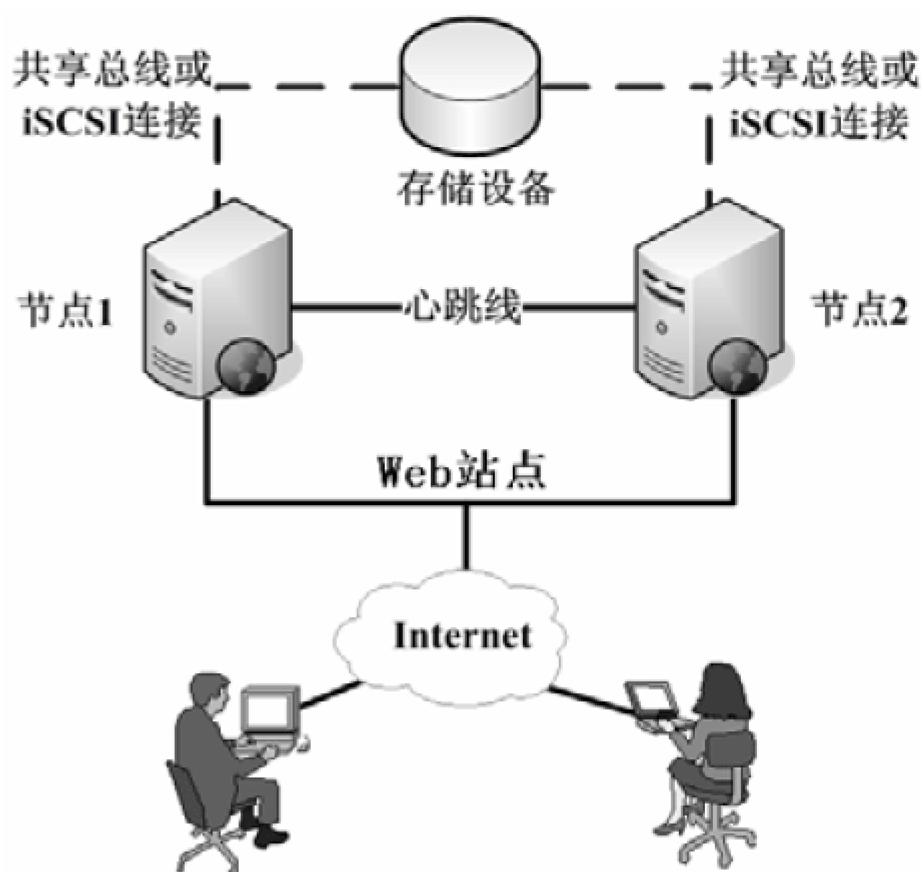


图 14-2　双节点的故障转移群集

从图 14-2 中可以看到，处于故障转移群集的两个节点通过心跳线和仲裁盘检测群集故障。心跳线，用于在各个节点定期交换数据报消息，如果备用节点在周期内没收到主动节点消息，会进行故障转移。仲裁磁盘用于保存群集配置数据库，可确保节点配置的一致性，确保任何群集资源只在

某一节点进入联机状态。

NLB 群集和故障转移群集具有很多差异，从服务种类、节点数目、操作系统需求等多方面比较可以构成表 14-1 所示的差异对照表。

表 14-1　NLB 群集和故障转移群集的差异

	NLB 群集	故障转移群集
服务种类	Web/FTP ISA VPN	SQL Server Exchange 文件和打印服务
最多节点数	32	8（X64 平台支持 16）
存储设备	不需要	需要
Windows Server 2008	所有版本	数据中心版 企业版

14.2　项目实战 1：配置 NLB 群集

NLB 群集的配置相对比较简单，本节将详细介绍 NLB 群集的准备、配置和验证等内容。

14.2.1　完成 NLB 群集的准备

在实施 NLB 群集之前首先要了解网络负载平衡需求，确定群集联网拓扑结构，具体内容介绍如下。

1. 案例需求分析

某公司使用 IIS 搭建 Web 服务器，随着公司业务的不断扩展，客户访问量逐渐增多，导致原来的单一服务器请求响应越来越慢。直接升级该硬件服务器配置不一定能解决访问性能限制，而且还会浪费原来的服务器硬件设备。所以公司计划新增一台 Web 服务器，使其与原来的服务器构建网络负载平衡群集。两台服务器提供相同的网站内容，利用网络负载平衡技术，根据每台服务器的负载情况动态地分担网络访问请求。

2. 网络拓扑图

网络调整后，两台服务器可按如图 14-3 所示拓扑结构进行互连。

如图 14-3 所示，两台服务器分别需要两块网卡 NLB 和 LAN，其中 NLB 网卡用于实现两台服务器的网络负载平衡，LAN 网卡用于服务器被外网访问。

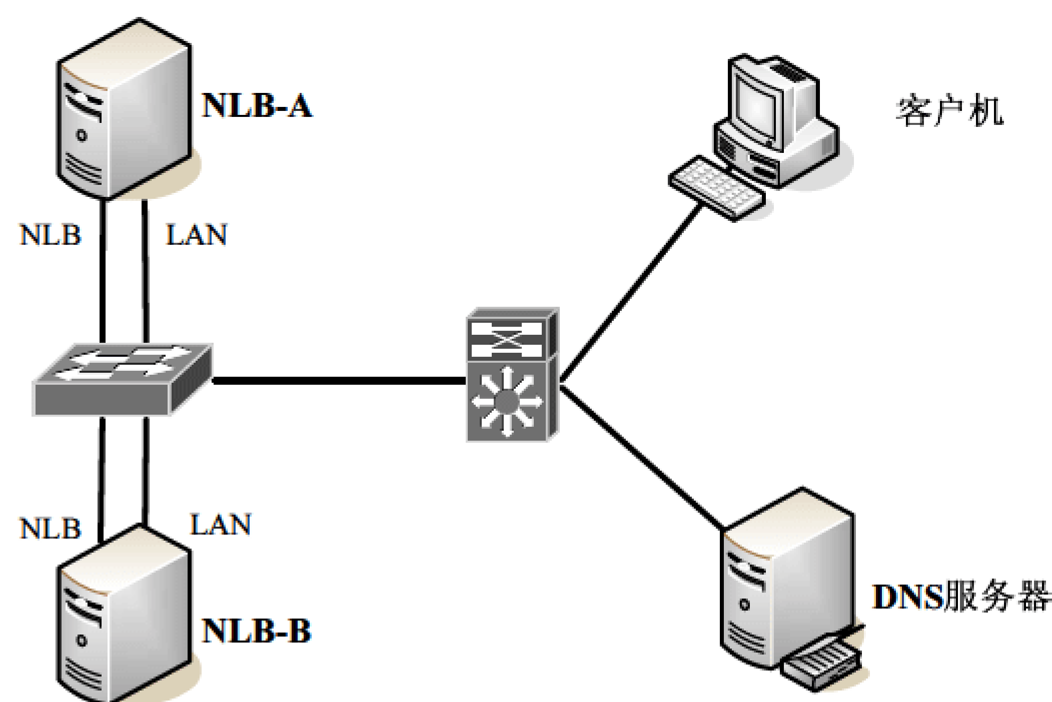


图 14-3　NLB 群集拓扑图

地址分配如表 14-2 所示。

表 14-2　　地址分配

NLB-A	NLB-B	DNS 服务器	客户机
LAN:192.168.1.11	LAN:192.168.1.12	192.168.1.254	192.168.1.100
NLB:192.168.10.1	NLB:192.168.10.2		

3. 在两台服务器上分别发布网站

网络拓扑连接好后，两台服务器需要分别构建 Web 发布环境以及安装 IIS，且有已发布的网站。由于是网络负载平衡，所以两台服务器发布的网站应该相同，本实例为了区分，在两台服务器上发布不同的网站，访问后的网站分别如图 14-4 和图 14-5 所示。



图 14-4　NLB-A 网站内容



图 14-5　NLB-B 网站内容

4. 配置 DNS 服务

需要为群集后的服务器配置 DNS 主机记录，该主机记录对应的 IP 地址应当为 NLB 群集后的访问地址，本实例采用“192.168.1.10”。DNS 主机记录解析的域名可结合实际情况自行定义，本实例采用“www.server.com”。

14.2.2　配置 NLB 群集

1. 安装网络负载平衡服务

需要在两台服务器上同时安装网络负载平衡功能，具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，选择左侧【功能】选项，如图 14-6 所示，在右侧单击【添加功能】链接。



图 14-6 【服务器管理器】窗口

02 弹出【添加功能向导】对话框，在【功能】选项列表中选中【网络负载平衡】选项，如图 14-7 所示，单击【下一步】按钮。

03 弹出【确认安装选择】对话框，如图 14-8 所示，单击【安装】按钮。

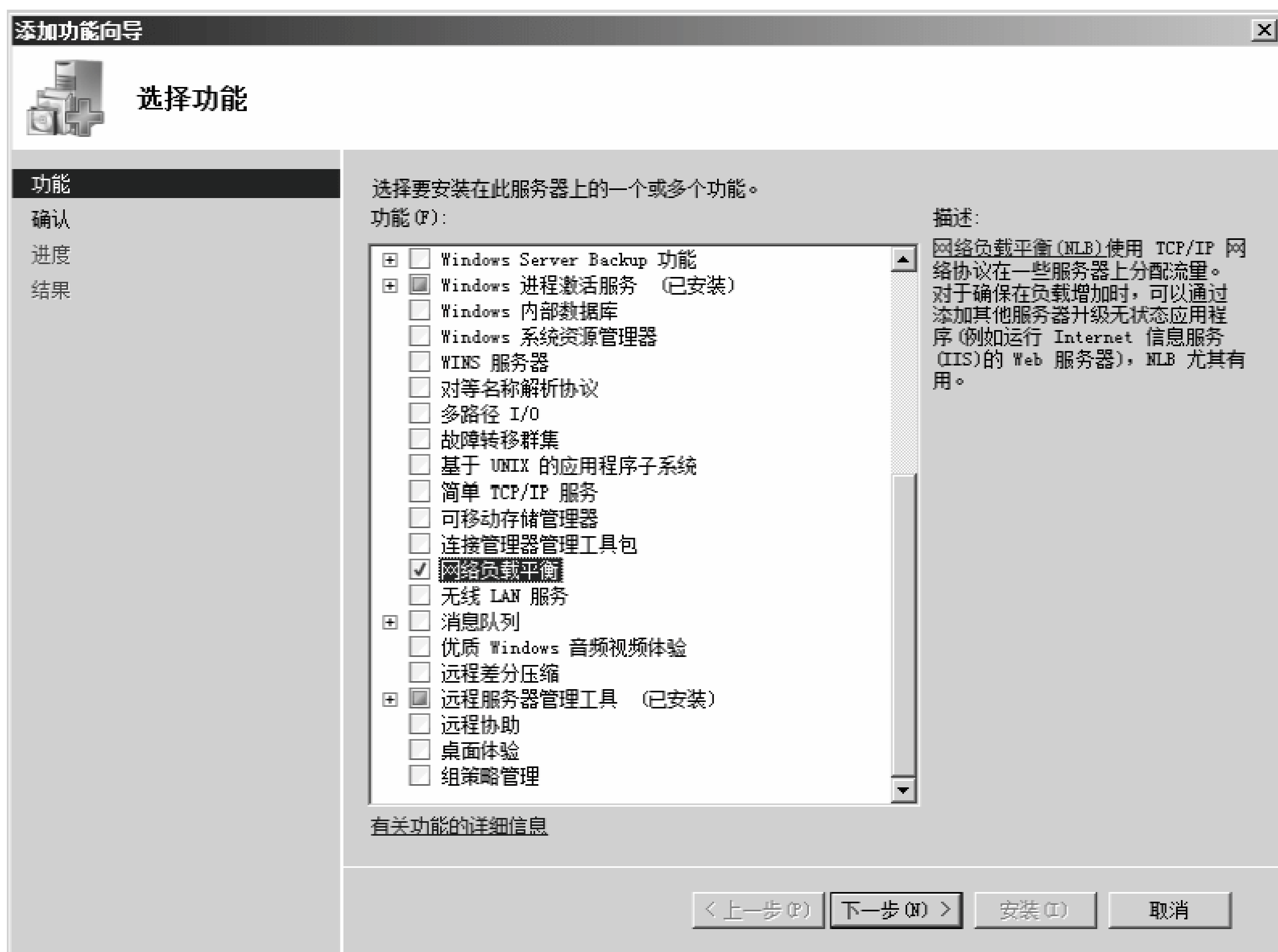


图 14-7 【添加功能向导】对话框



图 14-8 【确认安装选择】对话框

04 弹出【安装进度】对话框，系统自动安装网络负载平衡组件，如图 14-9 所示。

05 安装完成后弹出【安装结果】对话框，单击【关闭】按钮结束安装向导，如图 14-10 所示。



图 14-9 【安装进度】对话框



图 14-10　【安装结果】对话框

2. 启用 NLB-A 主机的网络负载平衡功能

首先需要在一台主机上新建群集，具体操作步骤如下。

01 选择【开始】➢【程序】➢【管理工具】➢【网络负载平衡管理器】命令，如图 14-11 所示。

02 弹出【网络负载平衡管理器】窗口，右击左侧【网络负载平衡群集】选项，在弹出的快捷菜单中选择【新建群集】命令，如图 14-12 所示。

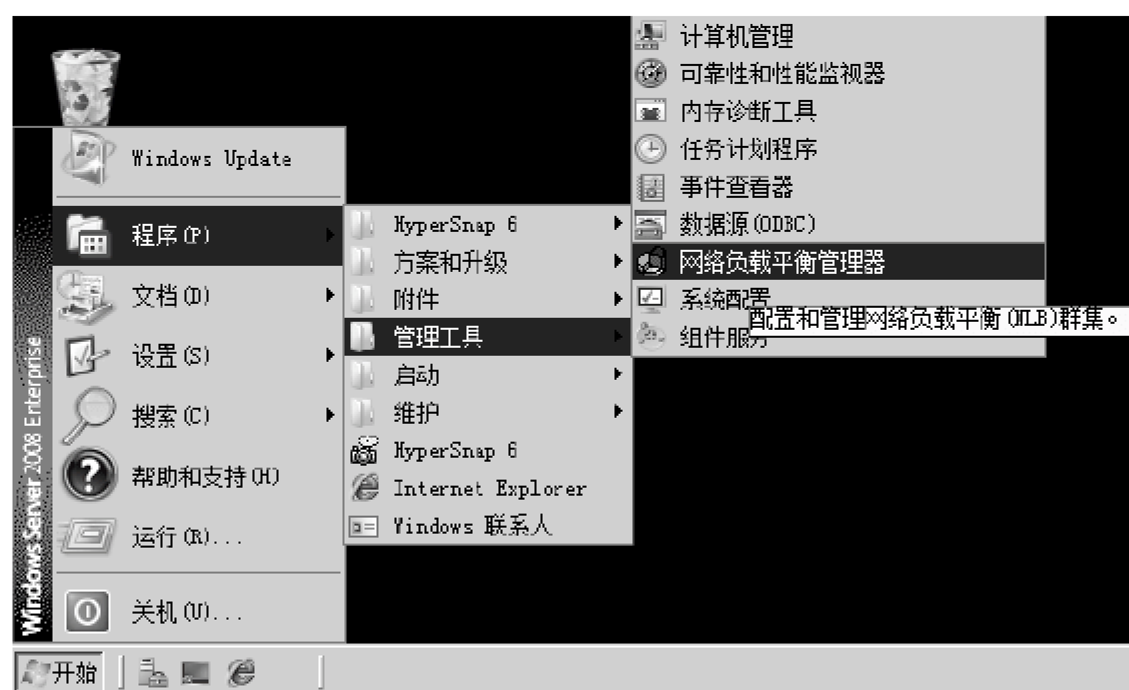


图 14-11　【网络负载平衡管理器】选项

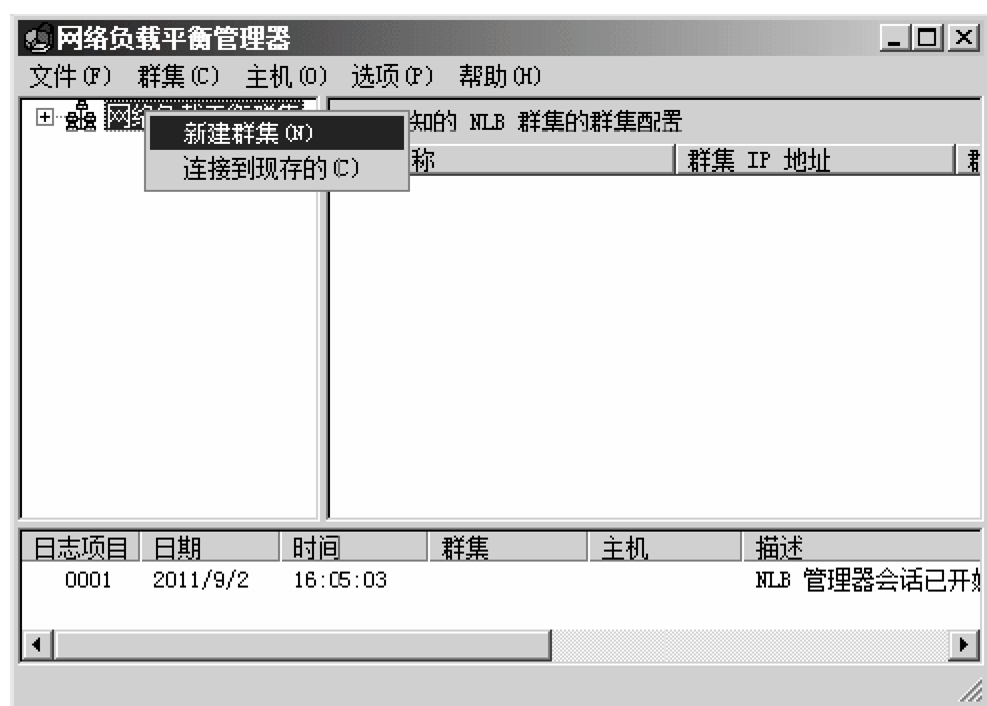


图 14-12　【网络负载平衡管理器】窗口

03 弹出【新群集：连接】对话框，在【主机】文本框中输入本服务器 NLB 网卡的 IP 地址，单击【连接】按钮，在【可用于配置新群集的接口】选项列表中显示出可用于选择的接口，选择【LAN】选项，单击【下一步】按钮，如图 14-13 所示。

04 弹出【新群集：主机参数】对话框，在【专用 IP 地址】选项列表中显示了局域网用于识别本机的 IP 地址和 LAN 网卡 IP 地址，其他采用默认配置，单击【下一步】按钮，如图 14-14 所示。

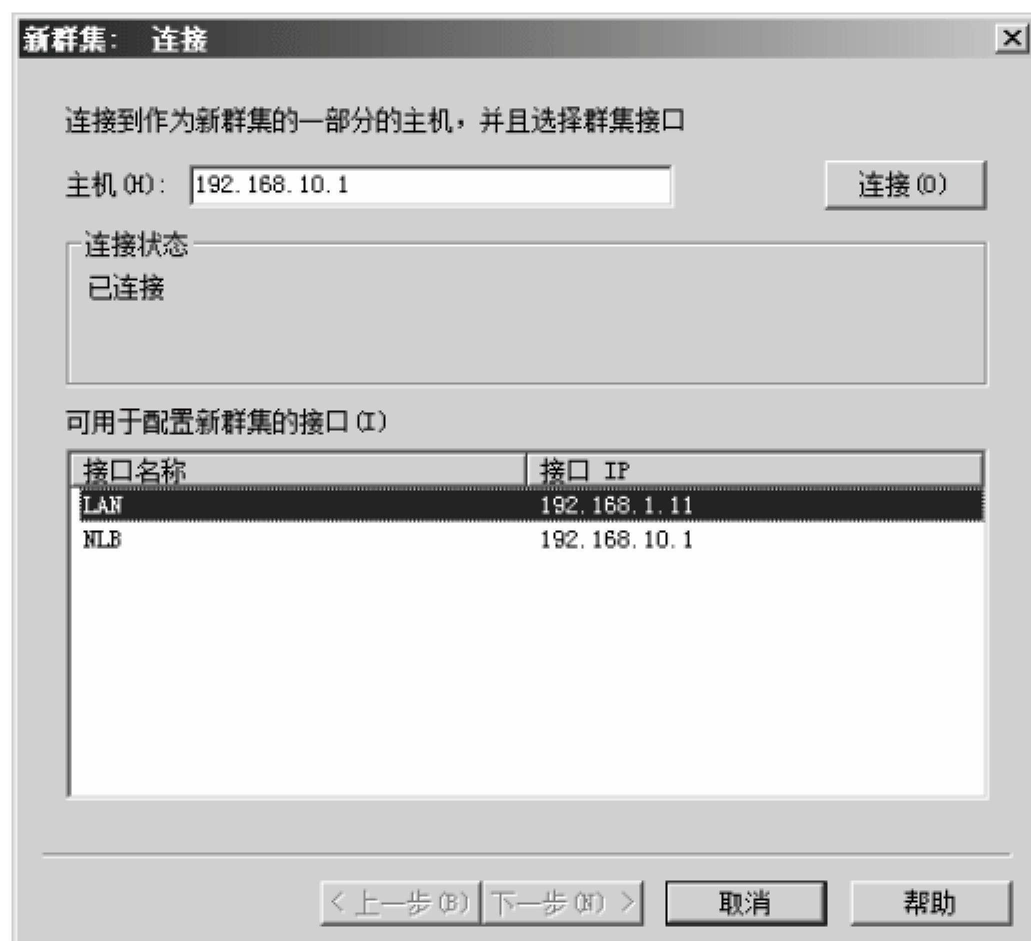


图 14-13 【新群集：连接】对话框



图 14-14 【新群集：主机参数】对话框

05 弹出【新群集：群集 IP 地址】对话框，该对话框用于设定两台服务器群集后共同使用的群集 IP 地址，单击【添加】按钮，如图 14-15 所示。

06 弹出【添加 IP 地址】对话框，本实例采用 IPv4 地址“192.168.1.10”，配置如图 14-16 所示，单击【确定】按钮。

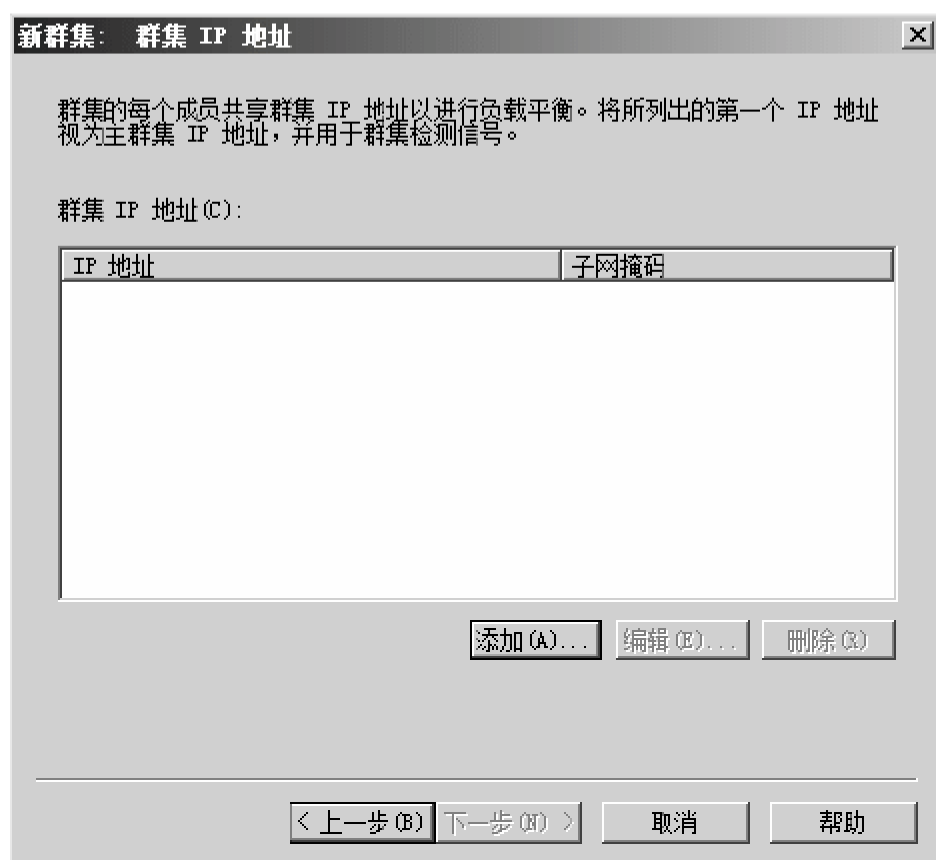


图 14-15 【新群集：群集 IP 地址】对话框

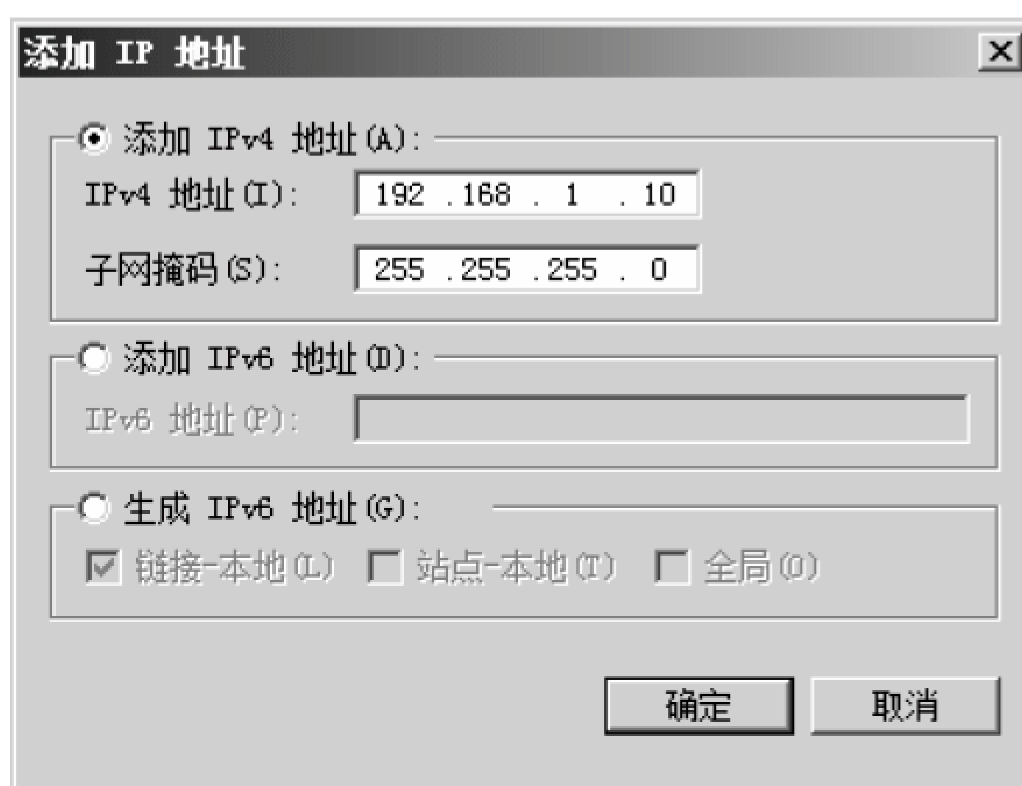


图 14-16 【添加 IP 地址】对话框

07 返回至【新群集：群集 IP 地址】对话框，在【群集 IP 地址】选项列表中显示了新添加的 IP 地址，单击【下一步】按钮，如图 14-17 所示。

08 弹出【新群集：群集参数】对话框，将【群集操作模式】修改为【多播】，其他采用默认配置，单击【下一步】按钮，如图 14-18 所示。

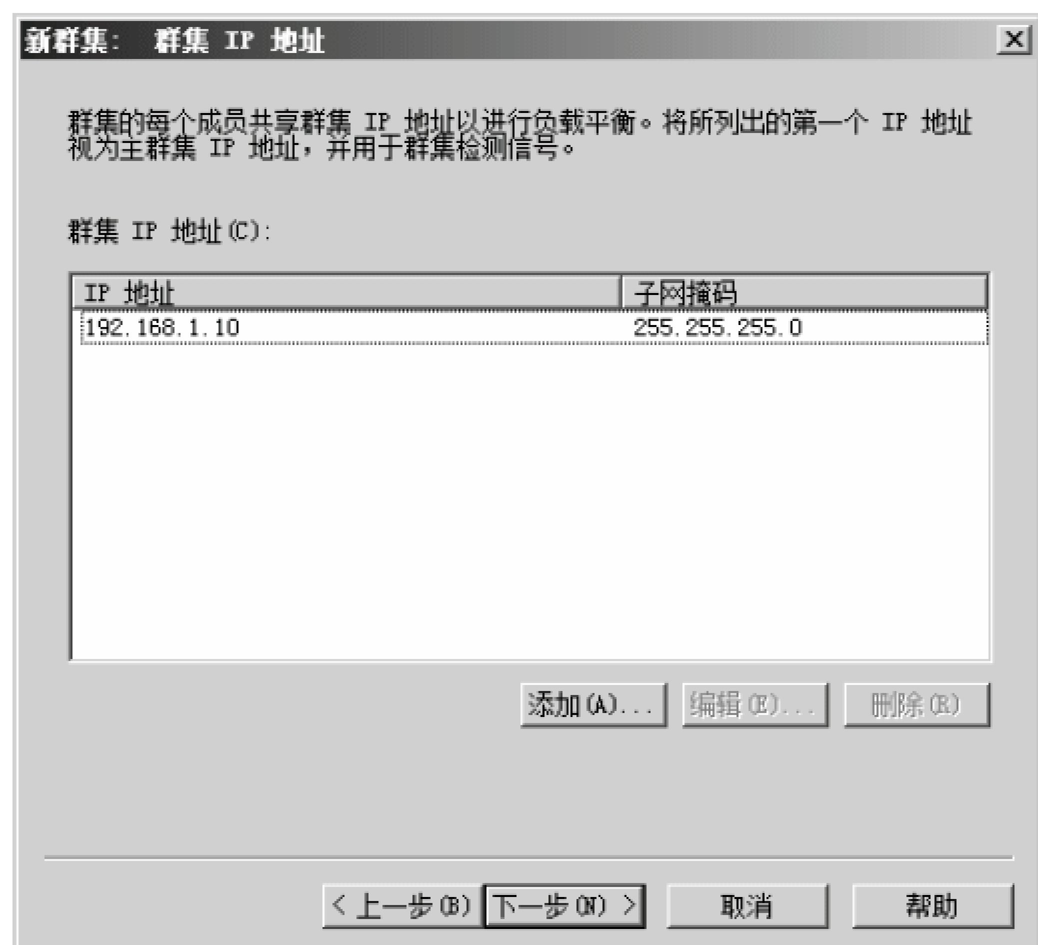


图 14-17　【新群集：群集 IP 地址】对话框



图 14-18　【新群集：群集参数】对话框

09 弹出【新群集：端口规则】对话框，在【定义的端口规则】选项列表中显示了 NLB 群集的端口规则，采用默认配置，单击【完成】按钮，如图 14-19 所示。

10 返回【网络负载平衡管理器】窗口，新添群集成功，并在下面显示日志信息，如图 14-20 所示。

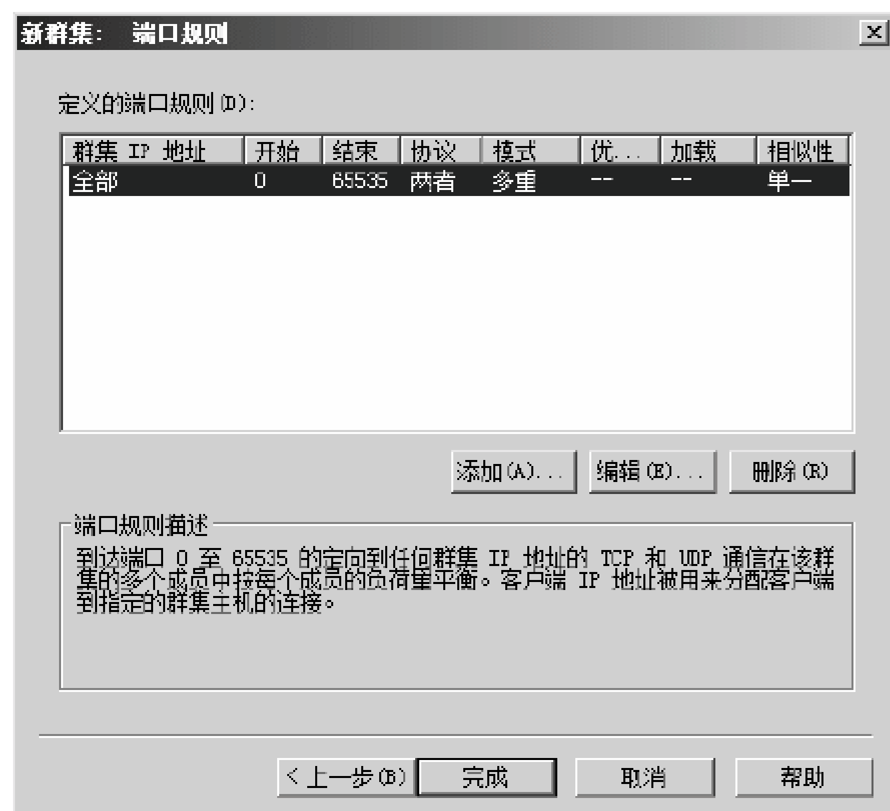


图 14-19　【新群集：端口规则】对话框



图 14-20　【网络负载平衡管理器】窗口

3. 将 NLB-B 连接到 NLB-A 创建的群集

当 NLB-A 群集创建好之后，NLB-B 直接进行连接即可，不需要重新创建新的群集，具体操作步骤如下。

01 选择【开始】➢【程序】➢【管理工具】➢【网络负载平衡管理器】命令。

02 弹出【网络负载平衡管理器】窗口，右击左侧【网络负载平衡群集】选项，在弹出的快捷菜单中选择【新建群集】命令。

03 弹出【连接到现有群集：连接】对话框，在【主机】文本框中输入 NLB-A 主机的 NLB 网卡地址“192.168.10.1”，单击【连接】按钮，当【群集】选项列表中显示有 NLB-A 主机创建的群集后，单击【下一步】按钮，如图 14-21 所示。

04 返回至【网络负载平衡管理器】窗口，可以看到 NLB-B 主机已连接到 NLB-A 创建的群集，如图 14-22 所示。



图 14-21 【连接到现有群集：连接】对话框

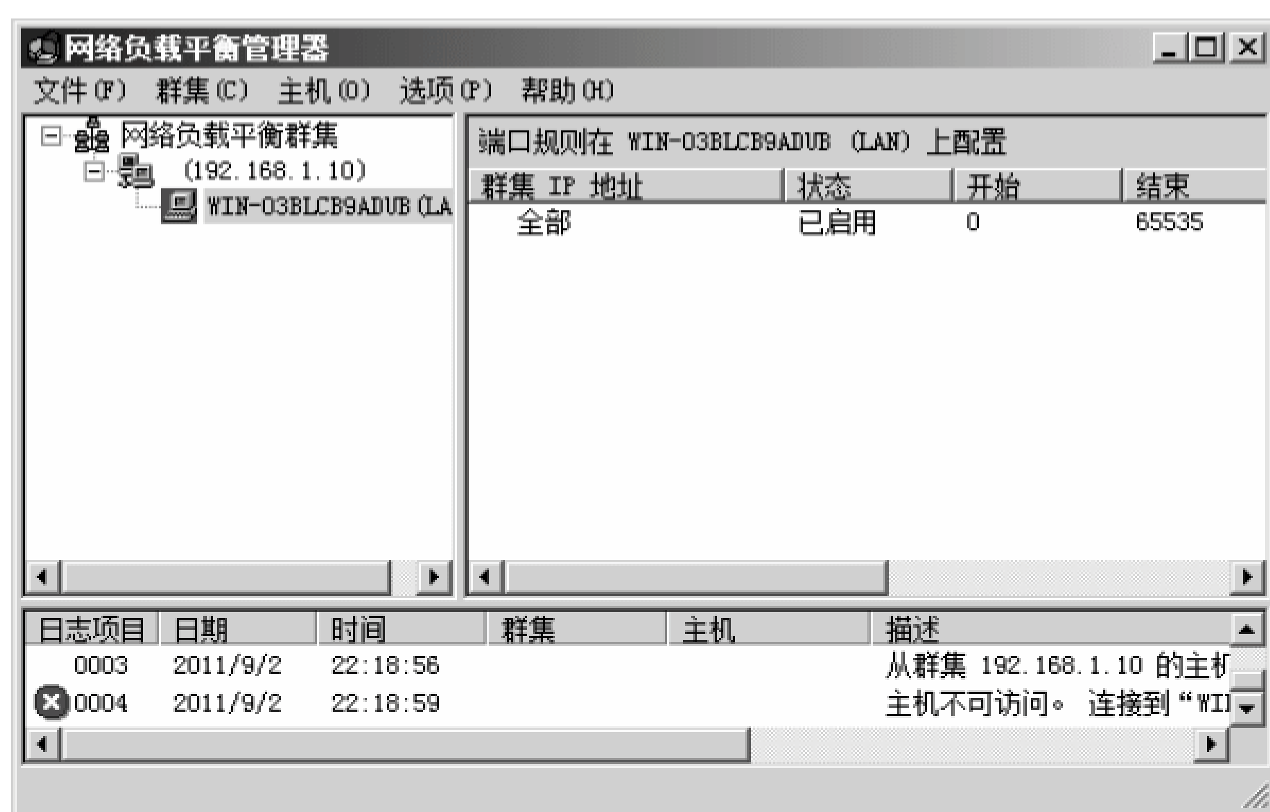


图 14-22 【网络负载平衡管理器】窗口

4. 添加 NLB-B 主机到群集

NLB-B 连接了 NLB-A 创建的群集后，还需要将 NLB-B 主机加入该群集，具体操作步骤如下。

01 在 NLB-B 主机中打开【网络负载平衡管理器】窗口，右击左侧选项中的【192.168.1.10】群集选项，在弹出的快捷菜单中选择【添加主机到群集】命令，如图 14-23 所示。

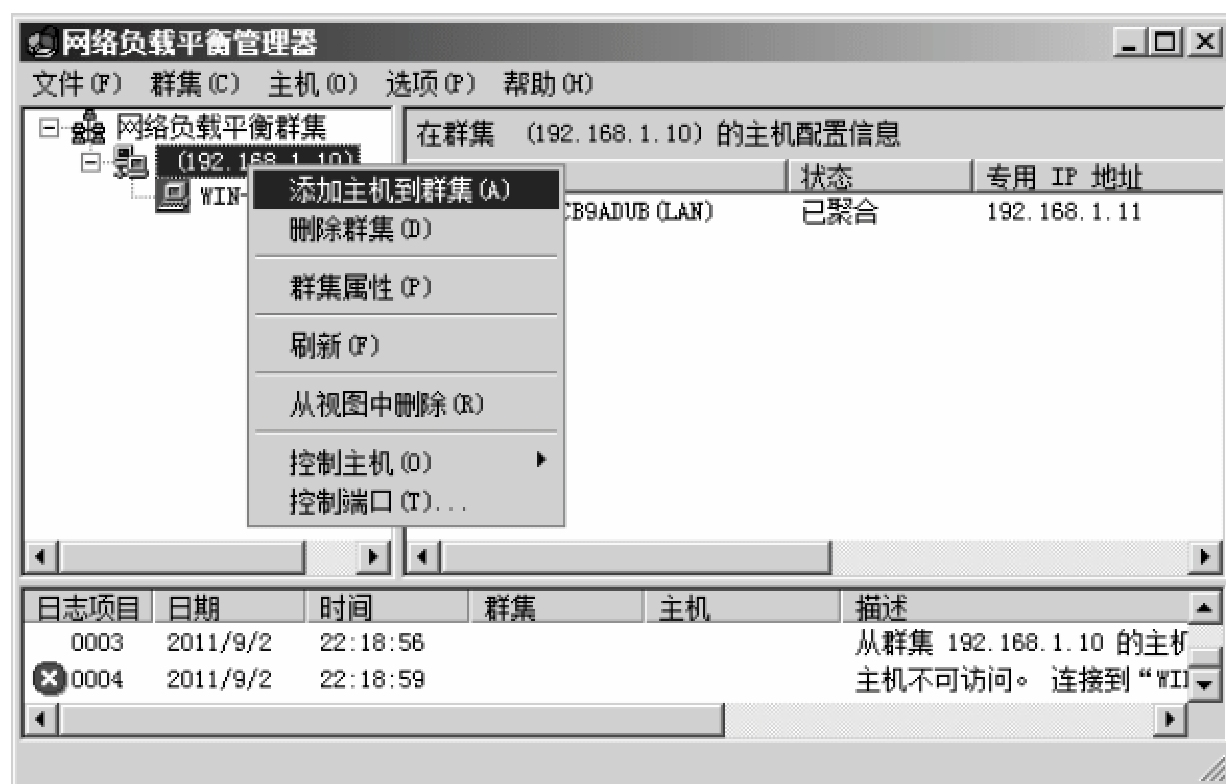


图 14-23 【网络负载平衡管理器】窗口

02 弹出【将主机添加到群集：连接】对话框，在【主机】文本框中输入 NLB-B 服务器的 NLB 网卡 IP 地址，单击【连接】按钮，在【可用于配置群集的接口】选项列表中显示出可用于选择的接口，选择【LAN】选项，单击【下一步】按钮，如图 14-24 所示。

03 弹出【将主机添加到群集：主机参数】对话框，在【专用 IP 地址】选项列表中显示了局域网用于识别本机的 IP 地址和 LAN 网卡 IP 地址，其他采用默认配置，单击【下一步】按钮，如图 14-25 所示。

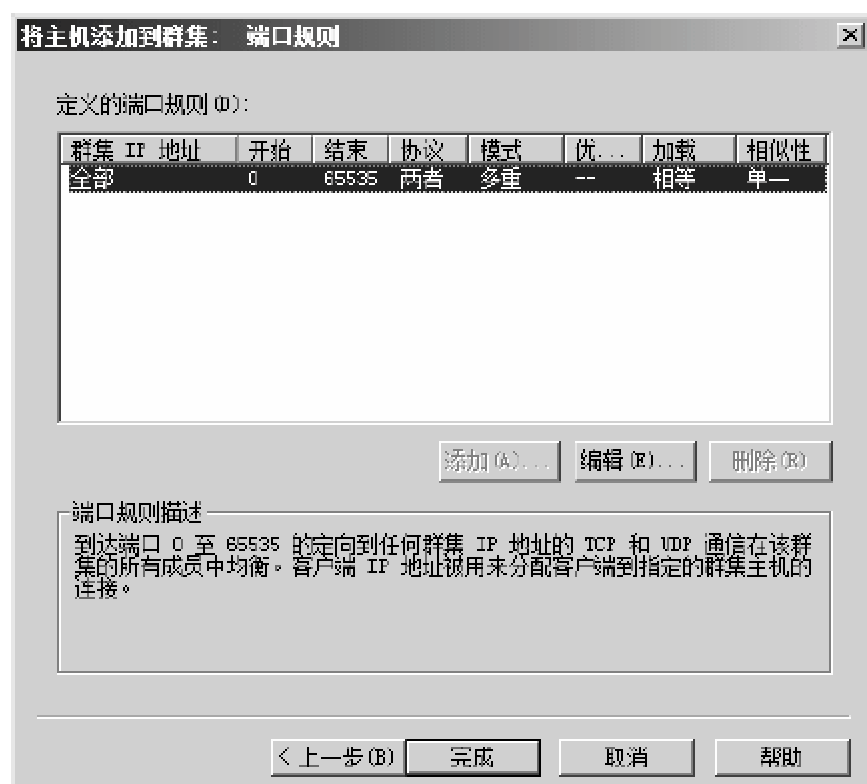




图 14-24　【将主机添加到群集：连接】对话框　　图 14-25　【将主机添加到群集：主机参数】对话框

04 弹出【将主机添加到群集：端口规则】对话框，在【定义的端口规则】选项列表中显示了 NLB 群集的端口规则，采用默认配置，单击【完成】按钮，如图 14-26 所示。

05 返回【网络负载平衡管理器】窗口，将主机 NLB-B 成功添加到群集中，如图 14-27 所示。



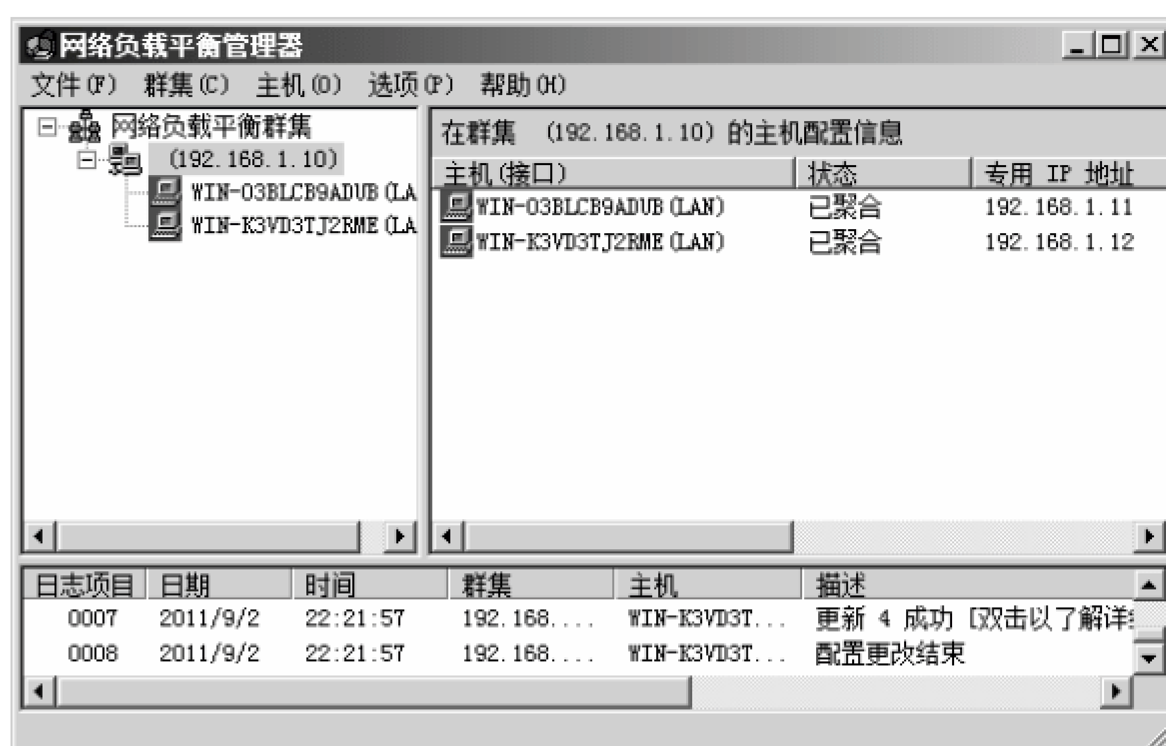


图 14-26　【将主机添加到群集：端口规则】对话框　　图 14-27　【网络负载平衡管理器】窗口

14.2.3　验证 NLB 群集

NLB 配置完成后，在客户机打开 IE 浏览器，输入域名“www.server.com”，如果 NLB-A 服务器响应访问请求，则显示如图 14-28 所示页面。



图 14-28　验证 NLB 群集 1

禁用 NLB-A 的网卡，此时 NLB-A 服务器已经无法被客户机访问到，客户机再次访问“www.server.com”网址，则会显示如图 14-29 所示页面，表示 NLB-B 起到了网络负载平衡的作用。



图 14-29　验证 NLB 群集 2



提　示

本实例构建网络负载平衡的两台服务器发布的网站不同，而实际网络环境下构建NLB群集的两台服务器发布的网站内容大都是相同的。

14.3　项目实战 2：创建故障转移群集

故障转移群集一般用于数据库、文件和打印服务、邮件服务等。本节将详细介绍配置故障转移群集前的准备、配置和验证内容。

14.3.1　完成故障转移群集的准备

配置故障转移群集前需要完成以下工作。

（1）为每个节点至少配备两块网卡，一块用于连接共享存储，一块用于网络通信，并且两个网卡不能使用同一网段地址。

（2）将群集中的所有节点服务器添加到同一个域环境中。

（3）配置有权限的管理账户，一般只要账户属于本地管理员，同时又属于 Domain User 组即可有群集的管理权限，不一定使用域管理员账户。

实验连接后的网络拓扑图如图 14-2 所示。

14.3.2　配置域环境

构建故障转移群集的服务器节点必须属于同一个域，所以首先要将节点加入到域中，具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，选择左侧【角色】选项，在右侧单击【添加角色】链接，如图 14-30 所示。

02 弹出【添加角色向导】对话框，如图 14-31 所示，单击【下一步】按钮。

03 弹出【选择服务器角色】对话框，如图 14-32 所示，选中【Active Directory 域服务】复选框，单击【下一步】按钮。



图 14-30 【服务器管理器】对话框

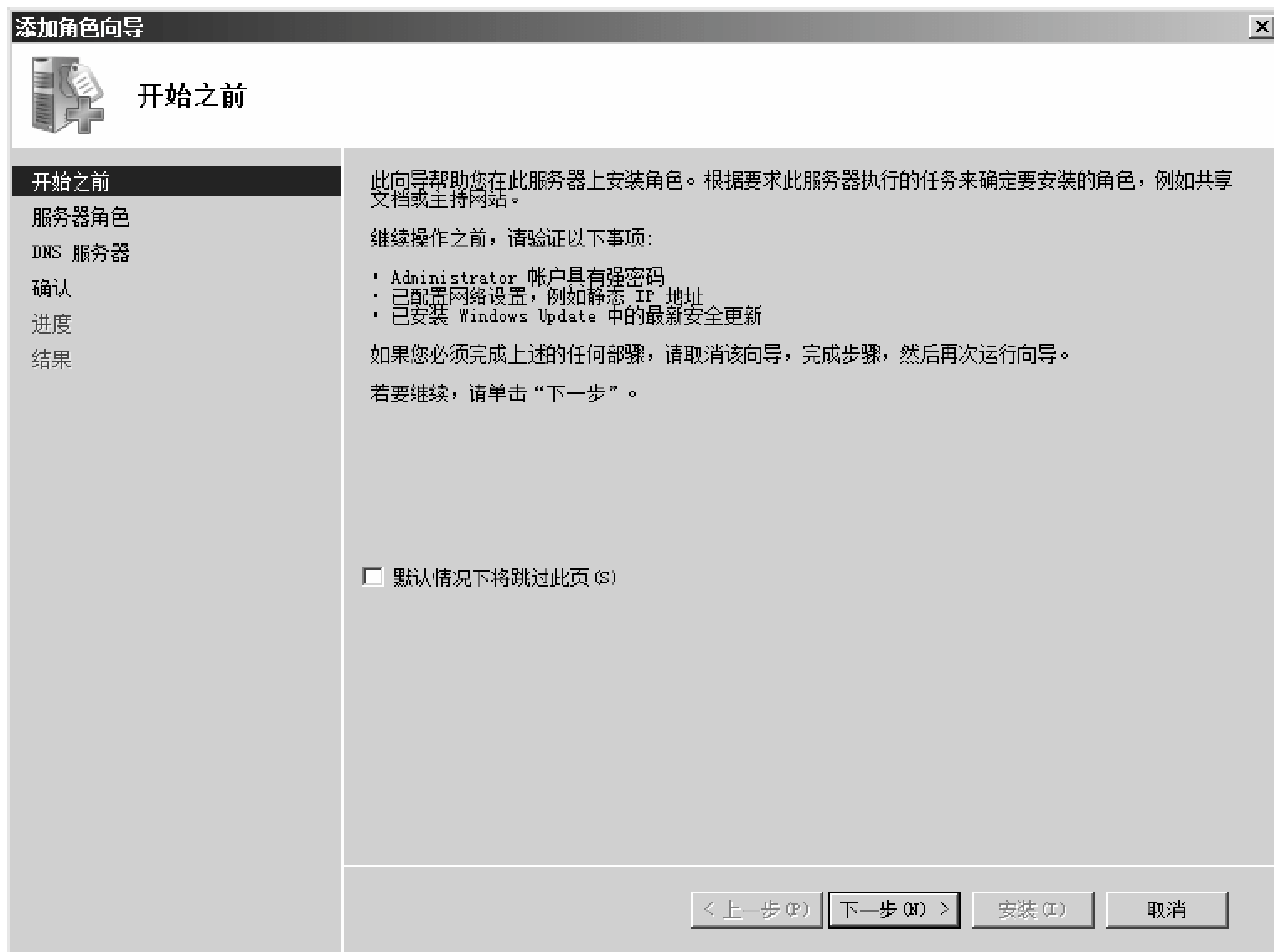


图 14-31 【添加角色向导】对话框

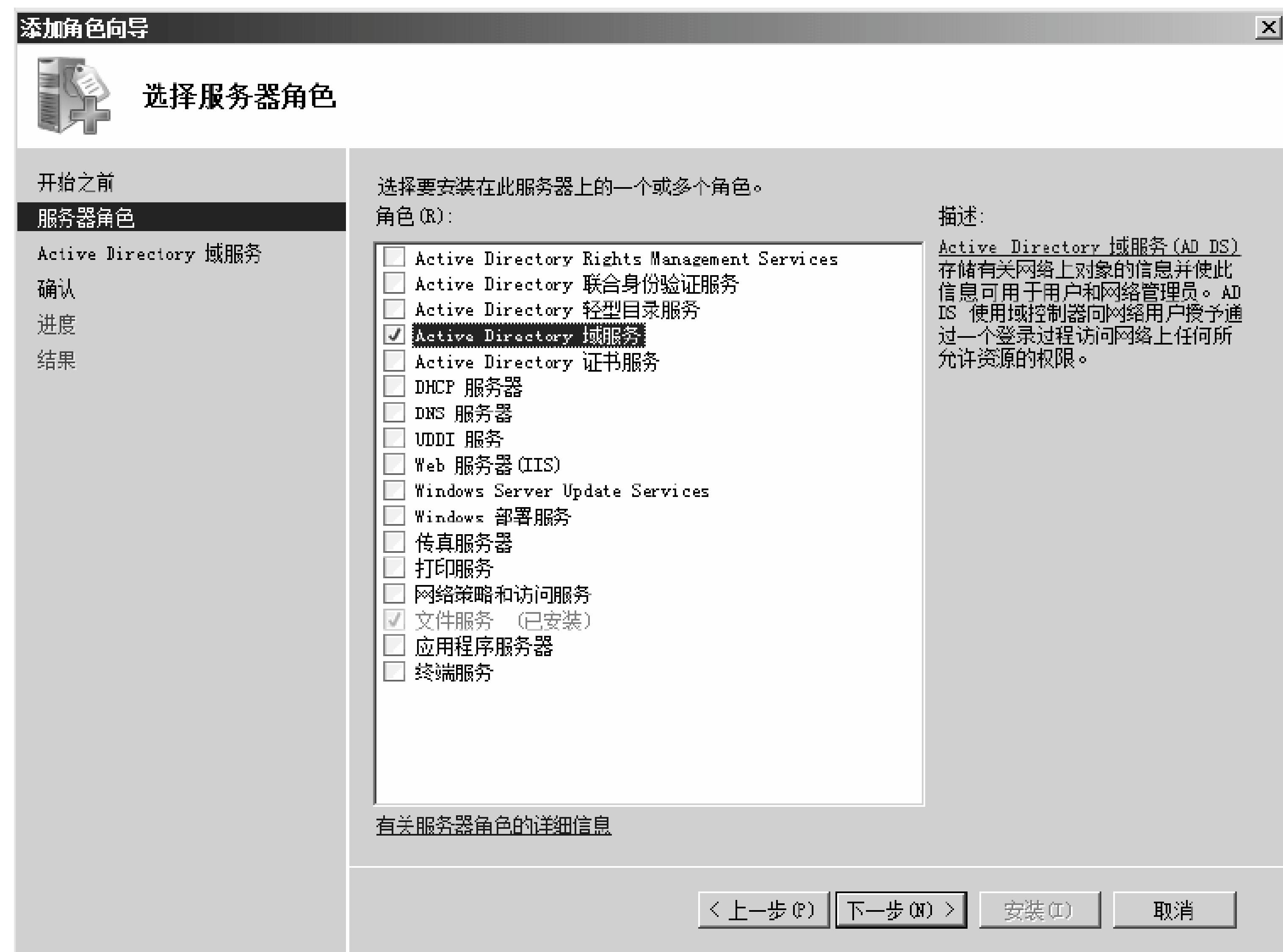


图 14-32 【选择服务器角色】对话框

04 弹出【Active Directory 域服务】对话框，显示了 DNS 服务器的介绍，单击【下一步】按钮，如图 14-33 所示。

05 弹出【确认安装选择】对话框，单击【安装】按钮，如图 14-34 所示。

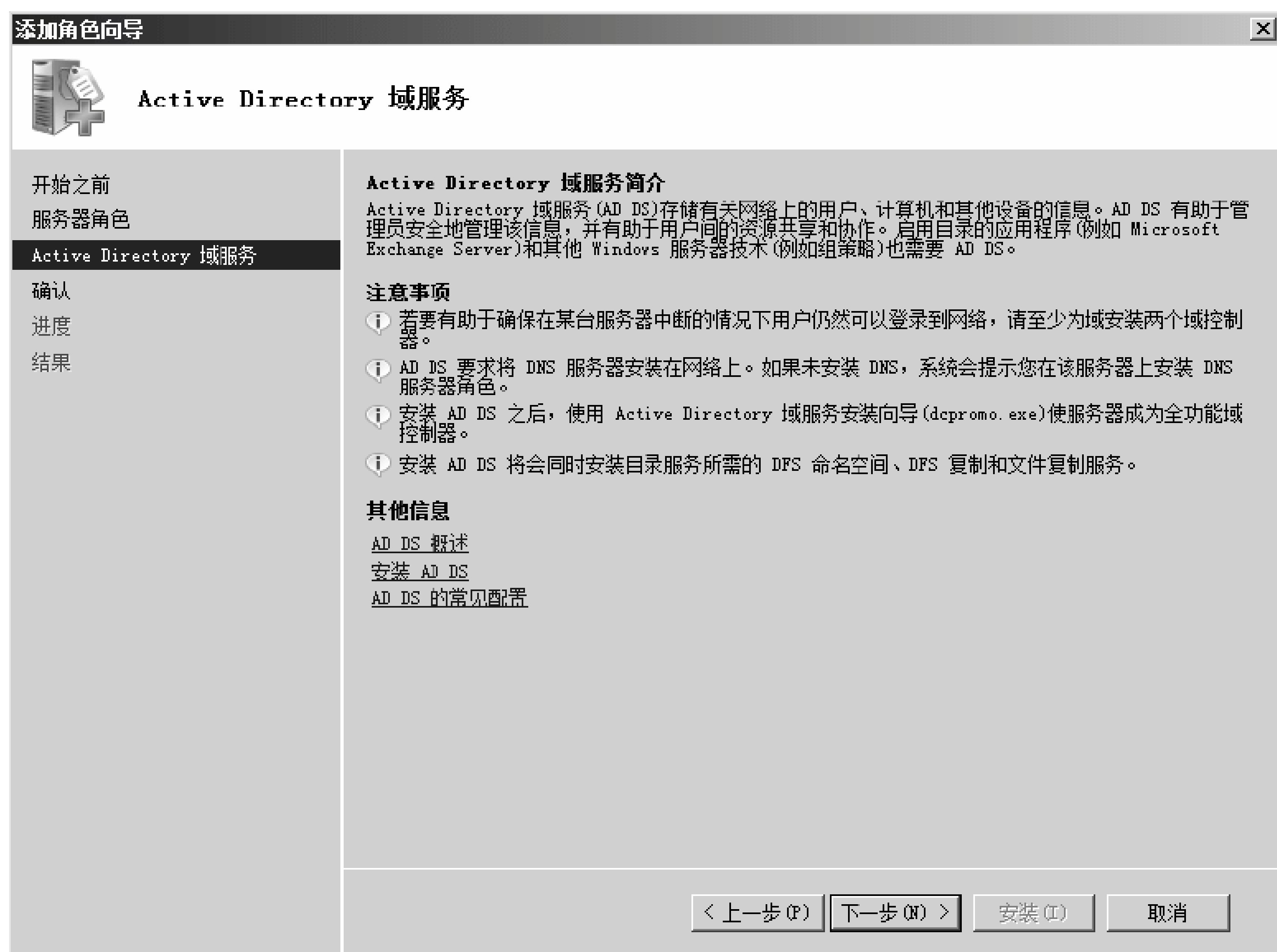


图 14-33 【Active Directory 域服务】对话框



图 14-34 【确认安装选择】对话框

06 弹出【安装进度】对话框，如图 14-35 所示。

07 弹出【安装结果】对话框，安装完成，单击【关闭】按钮，如图 14-36 所示。



图 14-35 【安装进度】对话框

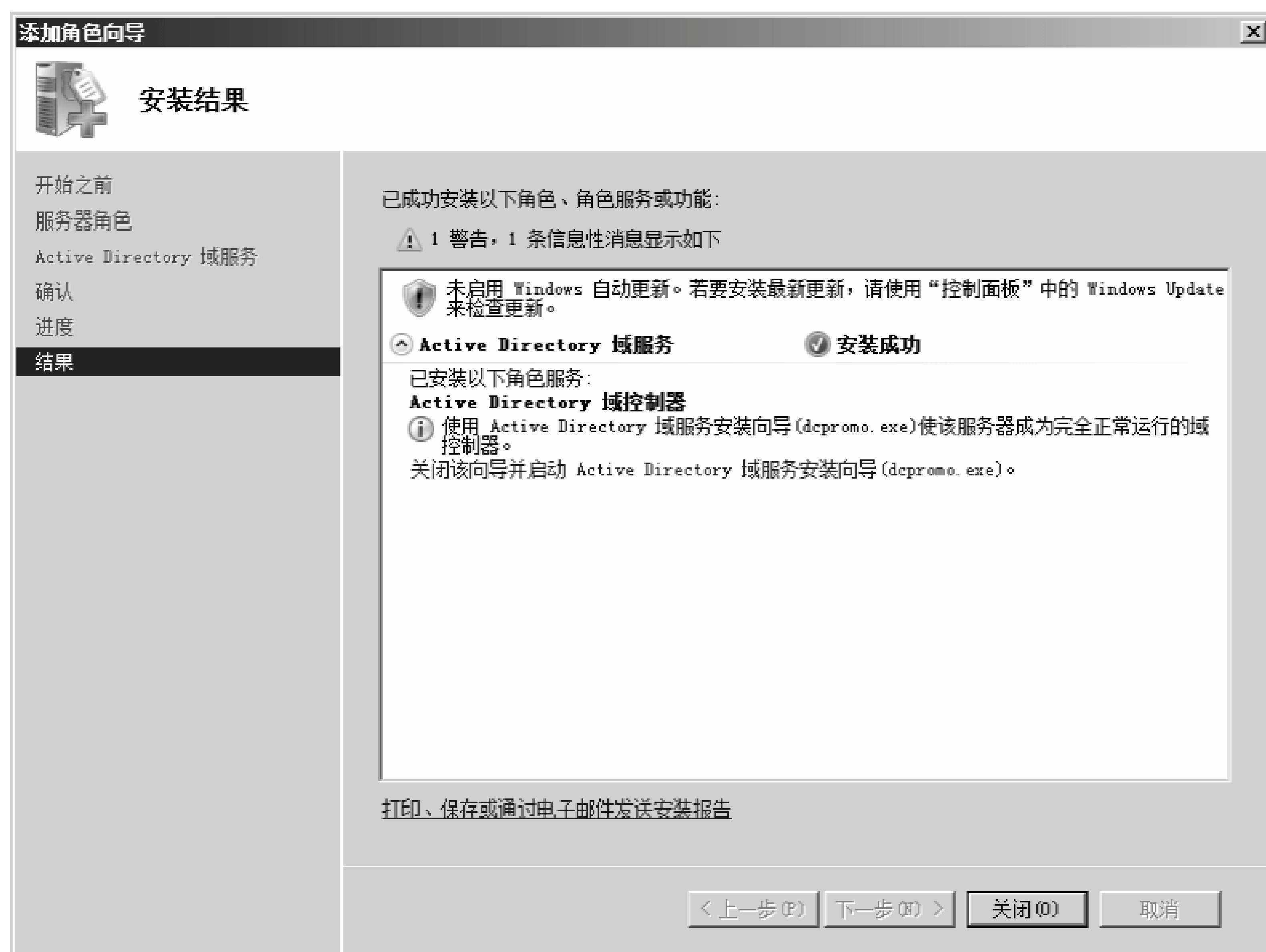


图 14-36 【安装结果】对话框

08 返回【服务器管理器】窗口，在左侧选项列表中选择【角色】➢【Active Directory 域服务】选项，在右侧【摘要】区域单击【运行 Active Directory 域服务安装向导】链接，如图 14-37 所示。



图 14-37 【服务器管理器】窗口

09 弹出安装向导对话框，单击【下一步】按钮，如图 14-38 所示。

10 弹出【操作系统兼容性】对话框，如果网络中有 Windows 旧版本的系统需要考虑兼容问题，单击【下一步】按钮，如图 14-39 所示。

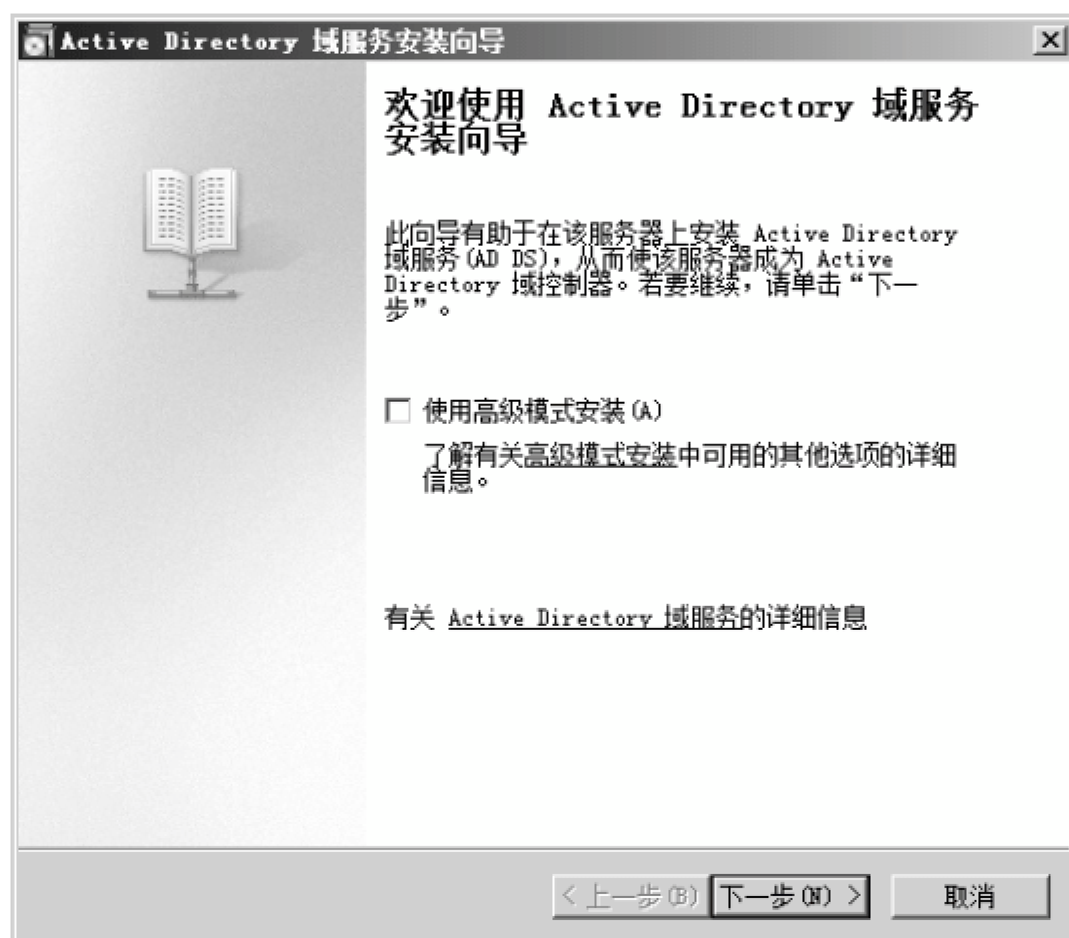




图 14-38 安装向导对话框

图 14-39 【操作系统兼容性】对话框

11 弹出【选择某一部署配置】对话框，本实例是新域，所以选中【在新林中新建域】单选按钮，单击【下一步】按钮，如图 14-40 所示。

12 弹出【命名林根域】对话框，在【目录林根级域的 FQDN】文本框中输入域的名称，本实例使用“yinhangit.com”，单击【下一步】按钮，如图 14-41 所示。

13 检测域名是否可用，如图 14-42 所示。

14 检测通过，弹出【设置林功能级别】对话框，主要有三种级别，本实例选择【Windows Server 2008】选项，单击【下一步】按钮，如图 14-43 所示。



图 14-40　【选择某一部署配置】对话框

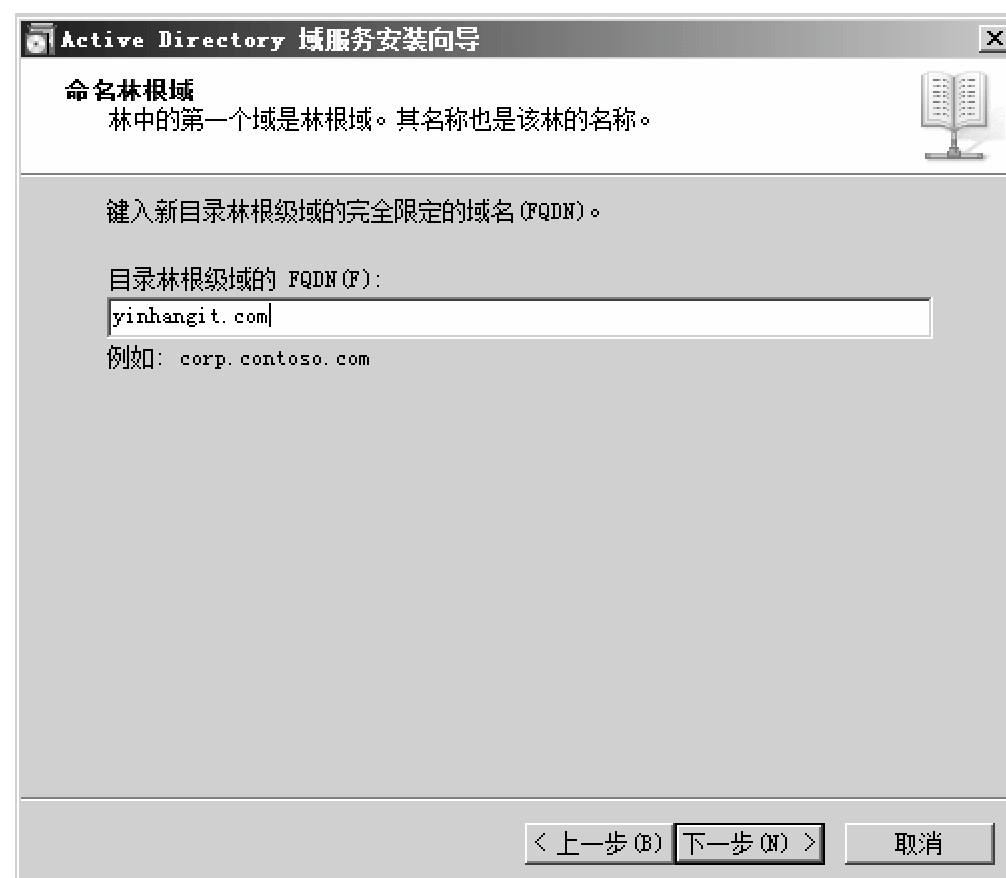


图 14-41　【命名林根域】对话框

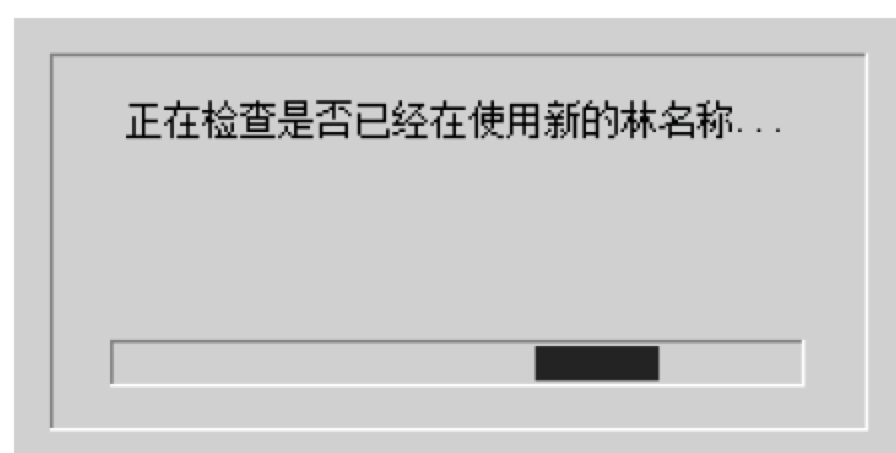


图 14-42　检测域名是否可用



图 14-43　【设置林功能级别】对话框

15 由于域环境需要 DNS 服务，所以安装前要检测 DNS 配置，如图 14-44 所示。

16 检测发现本地无 DNS 服务器，弹出【其他域控制器选项】对话框，选中【DNS 服务器】复选框，单击【下一步】按钮，如图 14-45 所示。

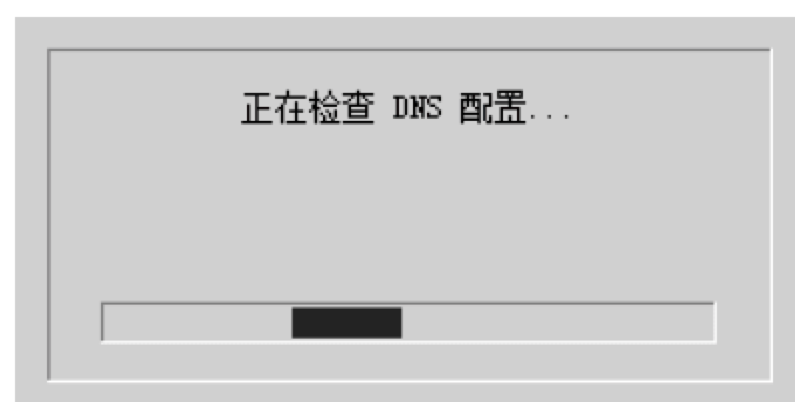


图 14-44　检测 DNS 配置

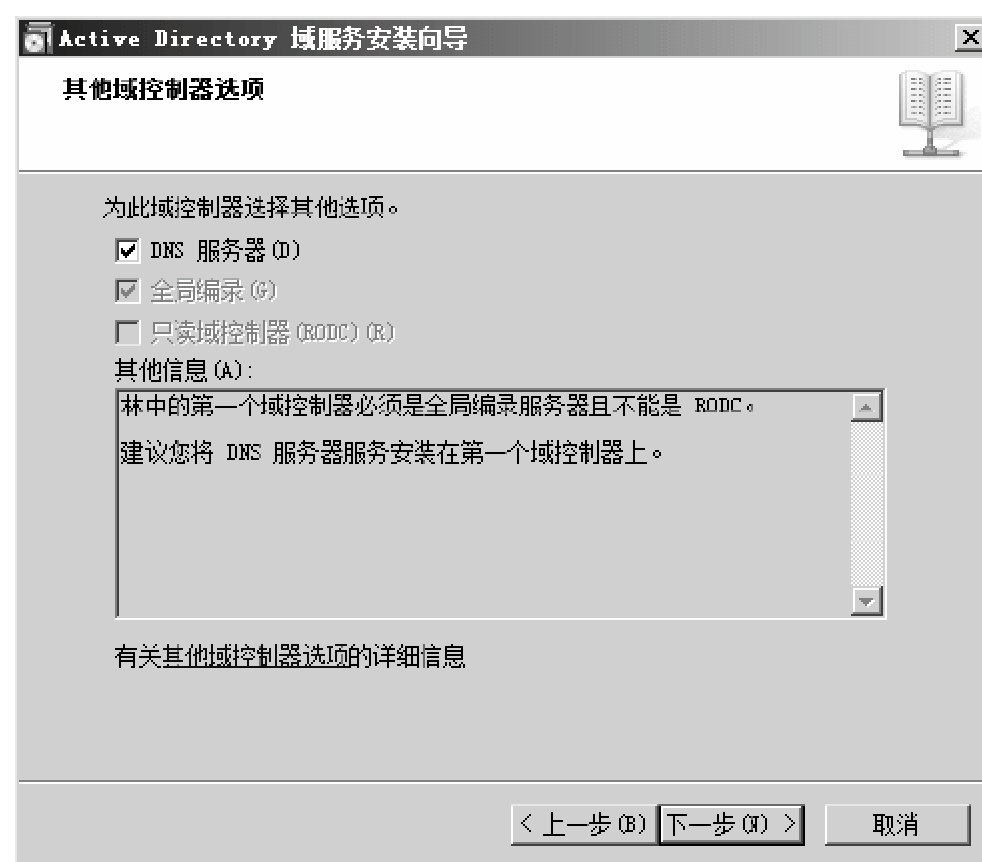


图 14-45　【其他域控制器选项】对话框

17 弹出【数据库、日志文件和 SYSVOL 的位置】对话框，可以分别指定数据库文件夹、日志文件文件夹、SYSVOL 文件夹的目录位置，本实例采用默认配置，单击【下一步】按钮，如图 14-46 所示。

18 弹出【目录服务还原模式的 Administrator 密码】对话框，当域故障以还原模式启动时，可用该密码进行登录，该密码和管理员账号密码无关。配置密码后单击【下一步】按钮，如图 14-47 所示。

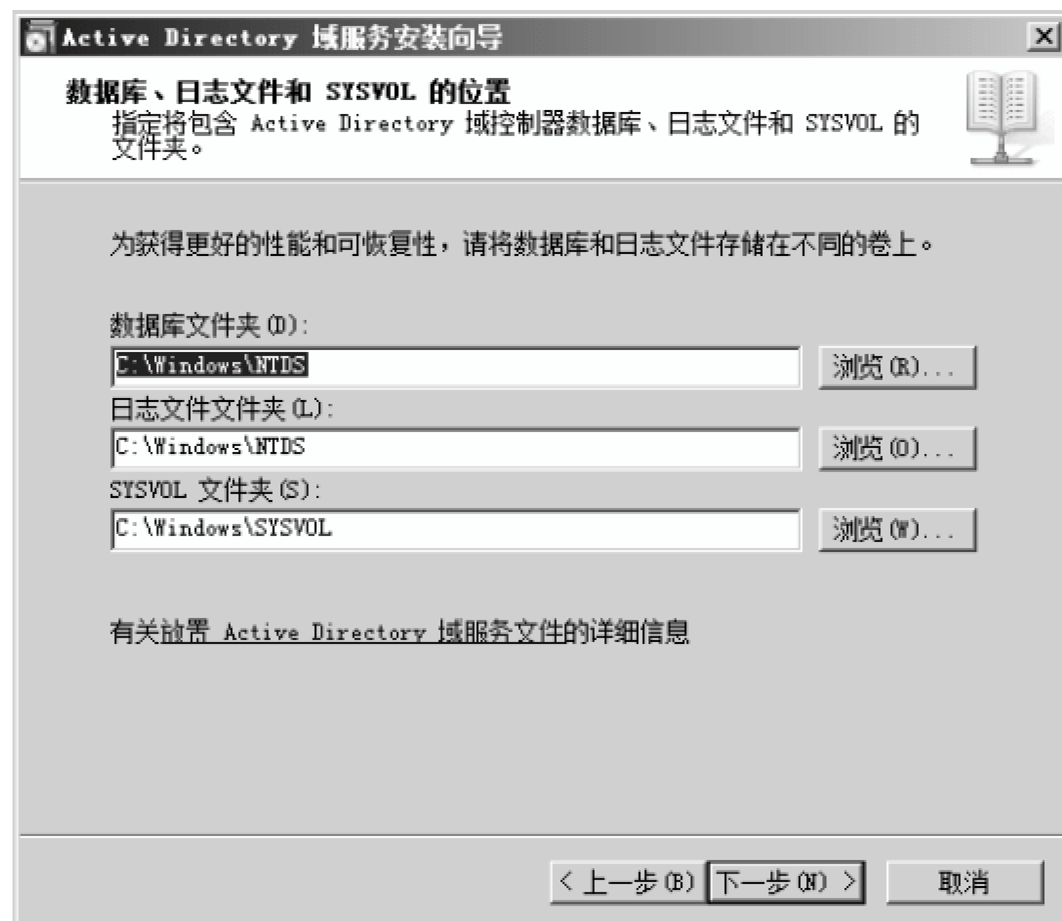


图 14-46 安装文件目录配置对话框

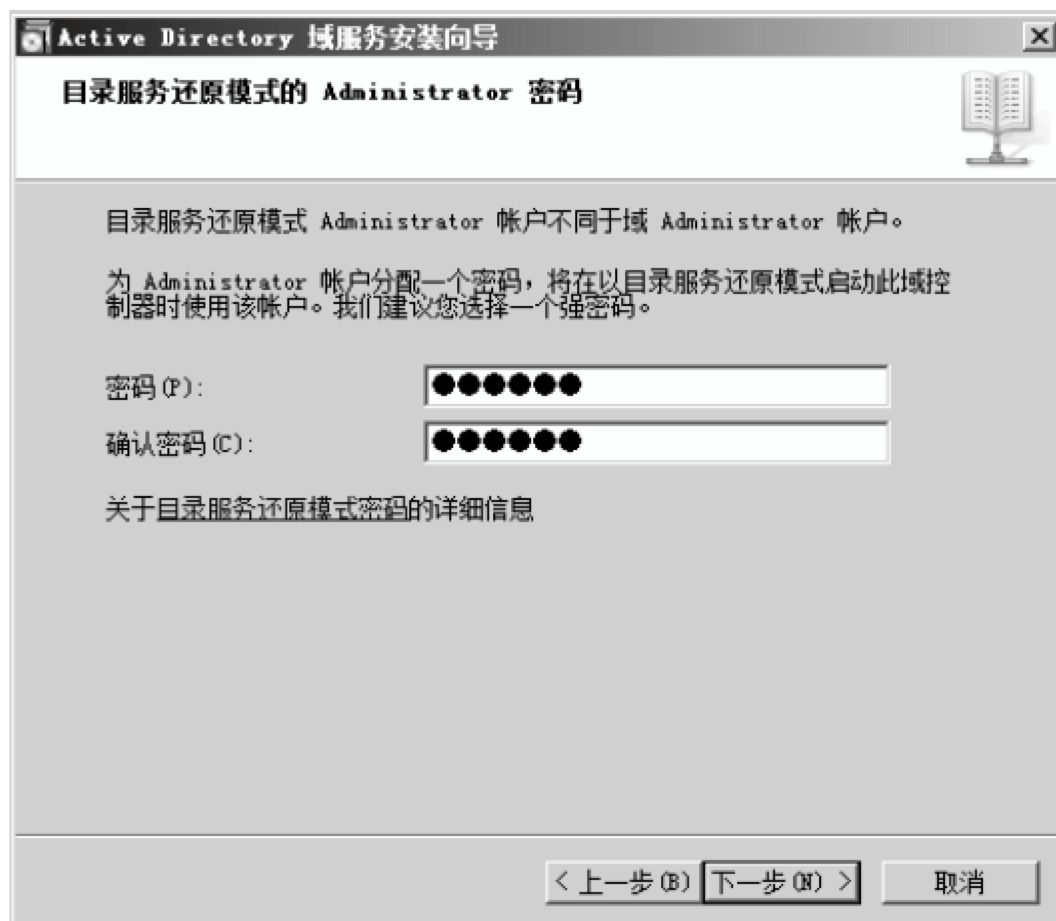


图 14-47 还原模式密码设置对话框

19 弹出【摘要】对话框，显示域控制器的配置信息，确认后单击【下一步】按钮，如图 14-48 所示。

20 开始安装域控制器的相关组件，如图 14-49 所示，可以单击【取消】按钮停止安装。



图 14-48 【摘要】对话框

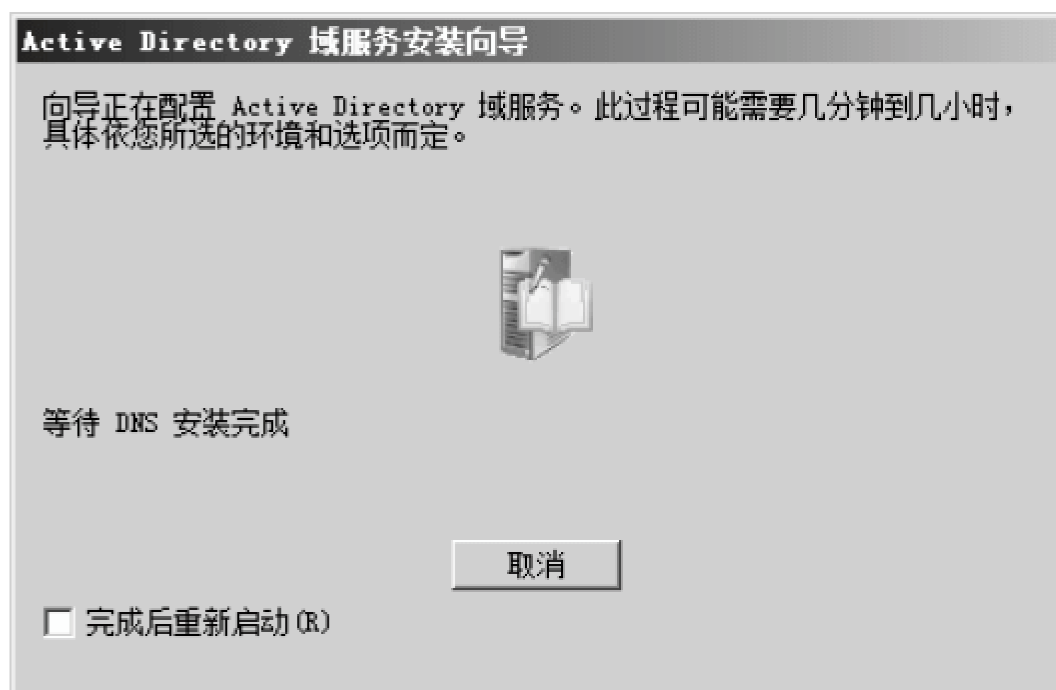


图 14-49 安装域控制器的相关组件

21 安装完成，弹出【完成 Active Directory 域服务安装向导】对话框，单击【完成】按钮，如图 14-50 所示。

22 弹出系统重启提示框，单击【立即重新启动】按钮使配置生效，如图 14-51 所示。



图 14-50　完成安装向导



图 14-51　系统重启提示框

另一个群集节点需要加入到该域中，操作方法同上。

14.3.3　安装故障转移群集

在 Windows Server 2008 中安装故障转移群集的具体操作步骤如下。

01 选择【开始】➢【管理工具】➢【服务器管理器】命令，弹出【服务器管理器】窗口，选择左侧【功能】选项，在右侧单击【添加功能】链接，如图 14-52 所示。



图 14-52　【服务器管理器】窗口

02 弹出【选择功能】对话框，选中【故障转移群集】复选框，单击【下一步】按钮，如图 14-53 所示。

03 弹出【确认安装选择】对话框，单击【安装】按钮，如图 14-54 所示。

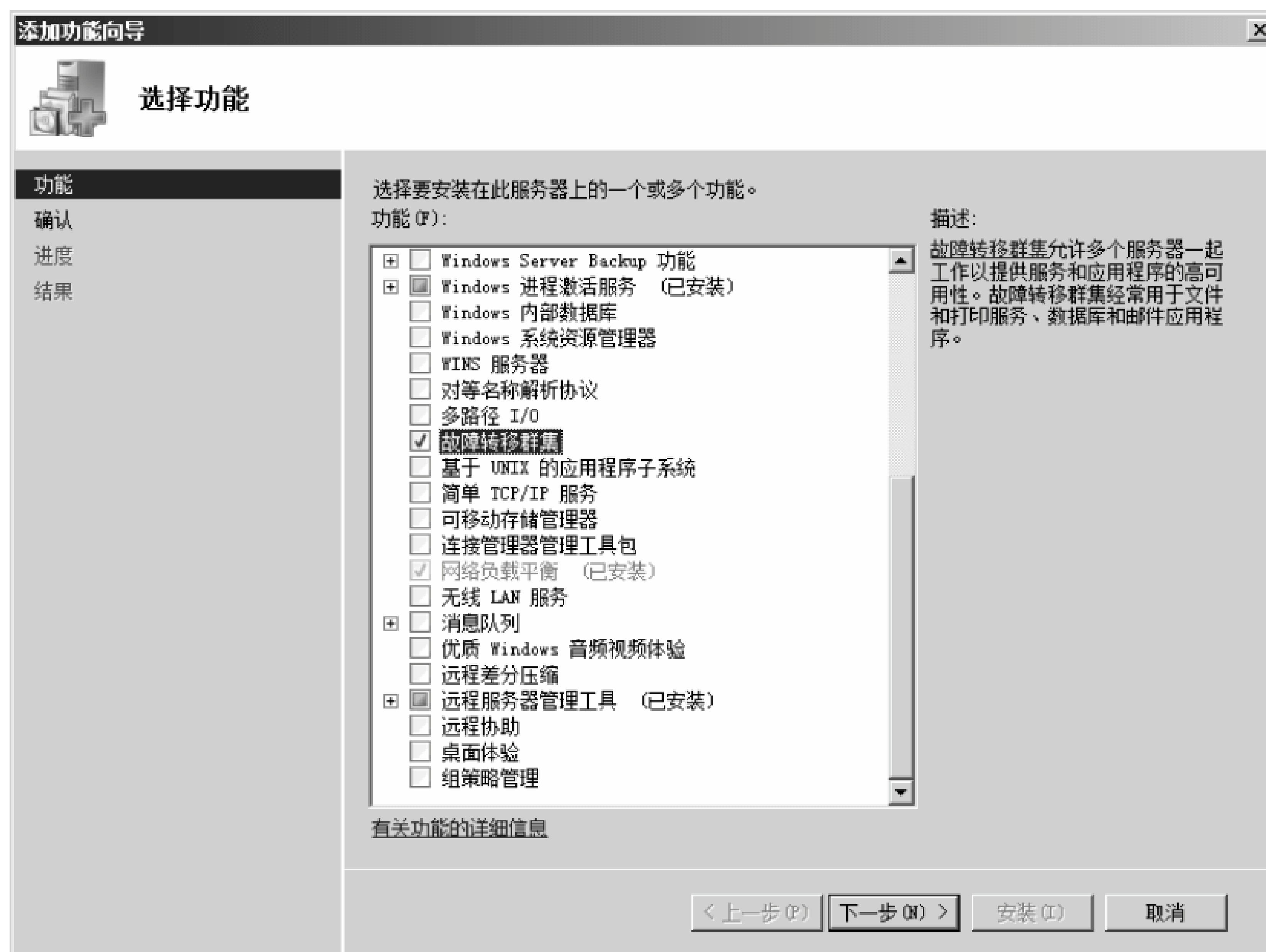


图 14-53 【选择功能】对话框



图 14-54 【确认安装选择】对话框

04 弹出【安装进度】对话框，如图 14-55 所示。

05 弹出【安装结果】对话框，安装完成，单击【关闭】按钮，如图 14-56 所示。



图 14-55 【安装进度】对话框



图 14-56 【安装结果】对话框

另外一个群集节点也要安装故障转移群集功能，操作方法同上。

14.3.4 验证故障转移群集配置

故障转移群集功能全部安装成功后，就可以创建群集了。但是为了确保群集成功，建议在创建群集之前运行验证群集配置，确认服务器、网络、存储是否符合要求。具体操作步骤如下。

01 选择【开始】➢【程序】➢【管理工具】➢【故障转移群集管理】选项，如图 14-57 所示。



图 14-57 【开始】菜单选项

02 打开【故障转移群集管理】窗口，在管理界面的中间位置单击【验证配置】链接，如图 14-58 所示。



图 14-58 【故障转移群集管理】窗口

03 弹出【开始之前】对话框，显示验证配置前的说明信息，单击【下一步】按钮，如图 14-59 所示。



图 14-59 【开始之前】对话框

04 弹出【请选择服务器或群集】对话框，在【输入名称】文本框中分别输入两个群集节点的计算机名称，单击【添加】按钮，如图 14-60 所示。



图 14-60　【请选择服务器或群集】对话框

05 两个群集节点添加成功，单击【下一步】按钮，如图 14-61 所示。



图 14-61　成功添加所有群集节点

06 弹出【正在测试选项】对话框，选择测试方式，默认选择【运行所有测试】单选按钮，单击【下一步】按钮，如图 14-62 所示。

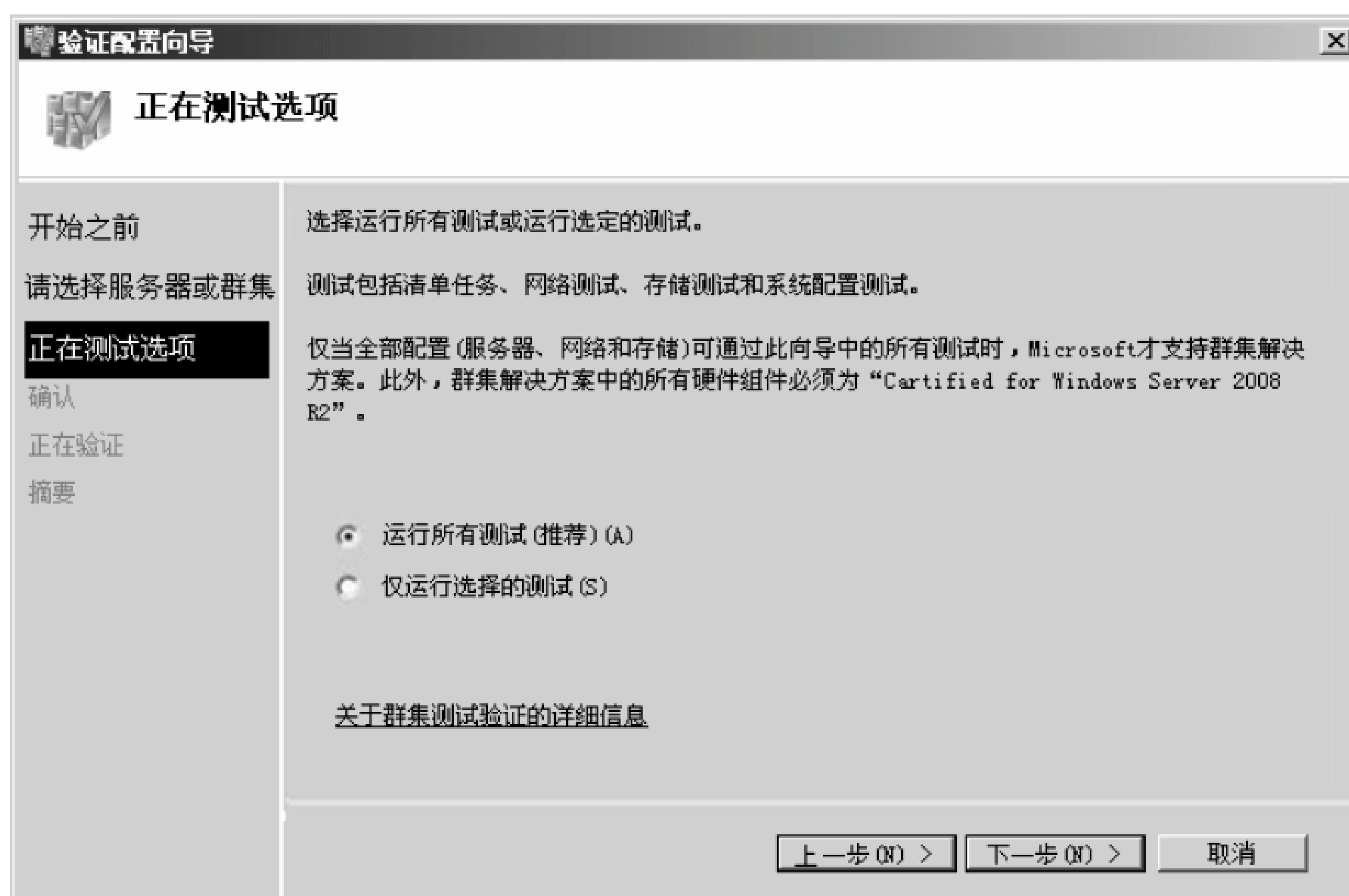


图 14-62 【正在测试选项】对话框

07 弹出【确认】对话框，显示了要进行测试的内容，单击【下一步】按钮，如图 14-63 所示。

08 弹出【正在验证】对话框，开始注意测试群集环境信息，可单击【取消】按钮结束测试，如图 14-64 所示。



图 14-63 【确认】对话框

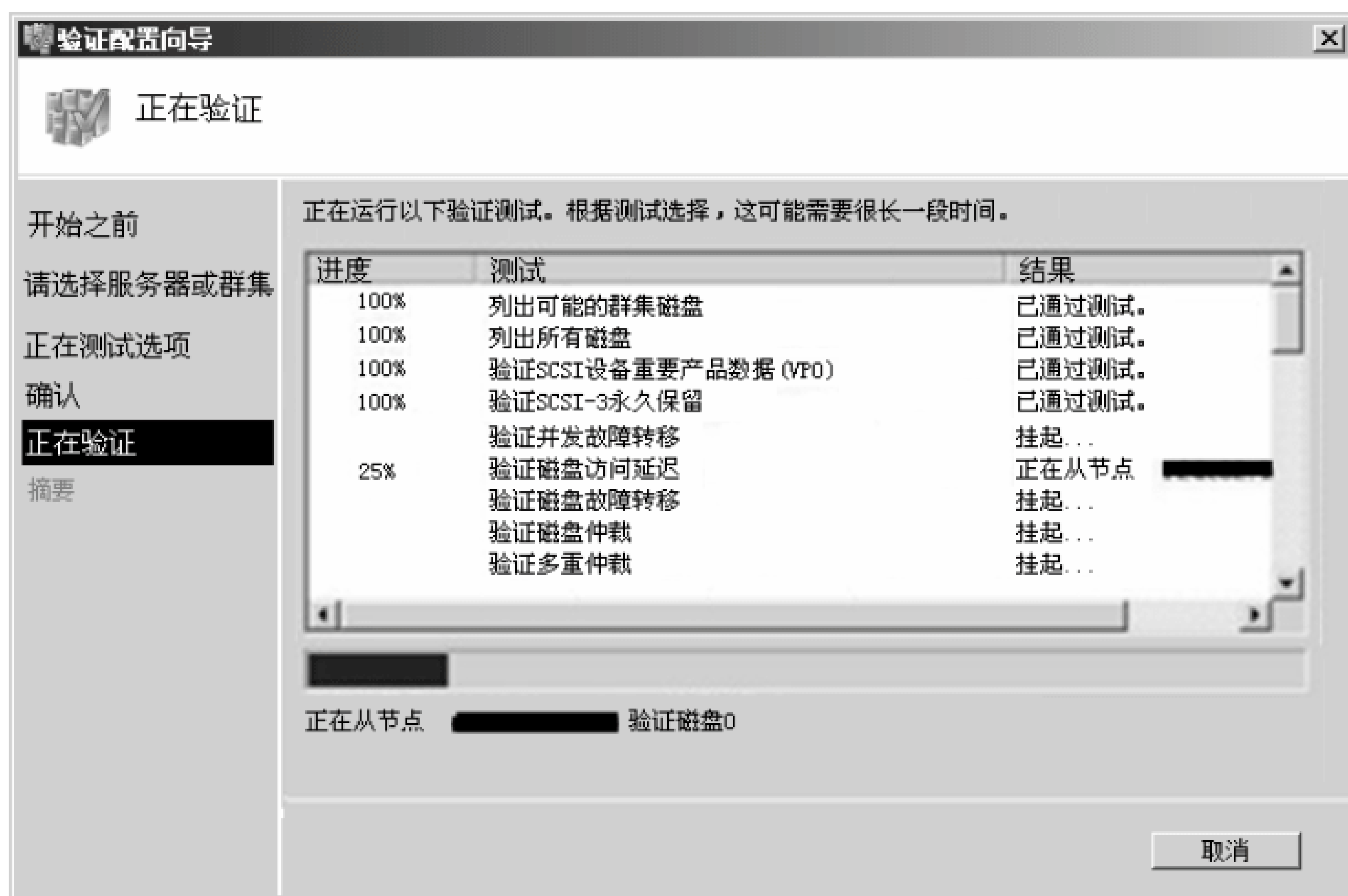


图 14-64　【正在验证】对话框

测试完成后会显示测试报告的查看链接，也可以在“C:\Windows\Cluster\Reports”目录下找到测试报告。

14.3.5　建立群集

测试完成后，就可以正式建立故障转移群集了，具体操作步骤如下。

01 打开【故障转移群集管理】窗口，在管理界面的中间位置单击【创建一个群集】链接，如图 14-65 所示。



图 14-65　【故障转移群集管理】窗口

02 弹出【开始之前】对话框，显示创建故障转移群集的相关说明信息，单击【下一步】按钮，如图 14-66 所示。

03 弹出【选择服务器】对话框，添加所有的群集节点，单击【下一步】按钮，如图 14-67 所示。

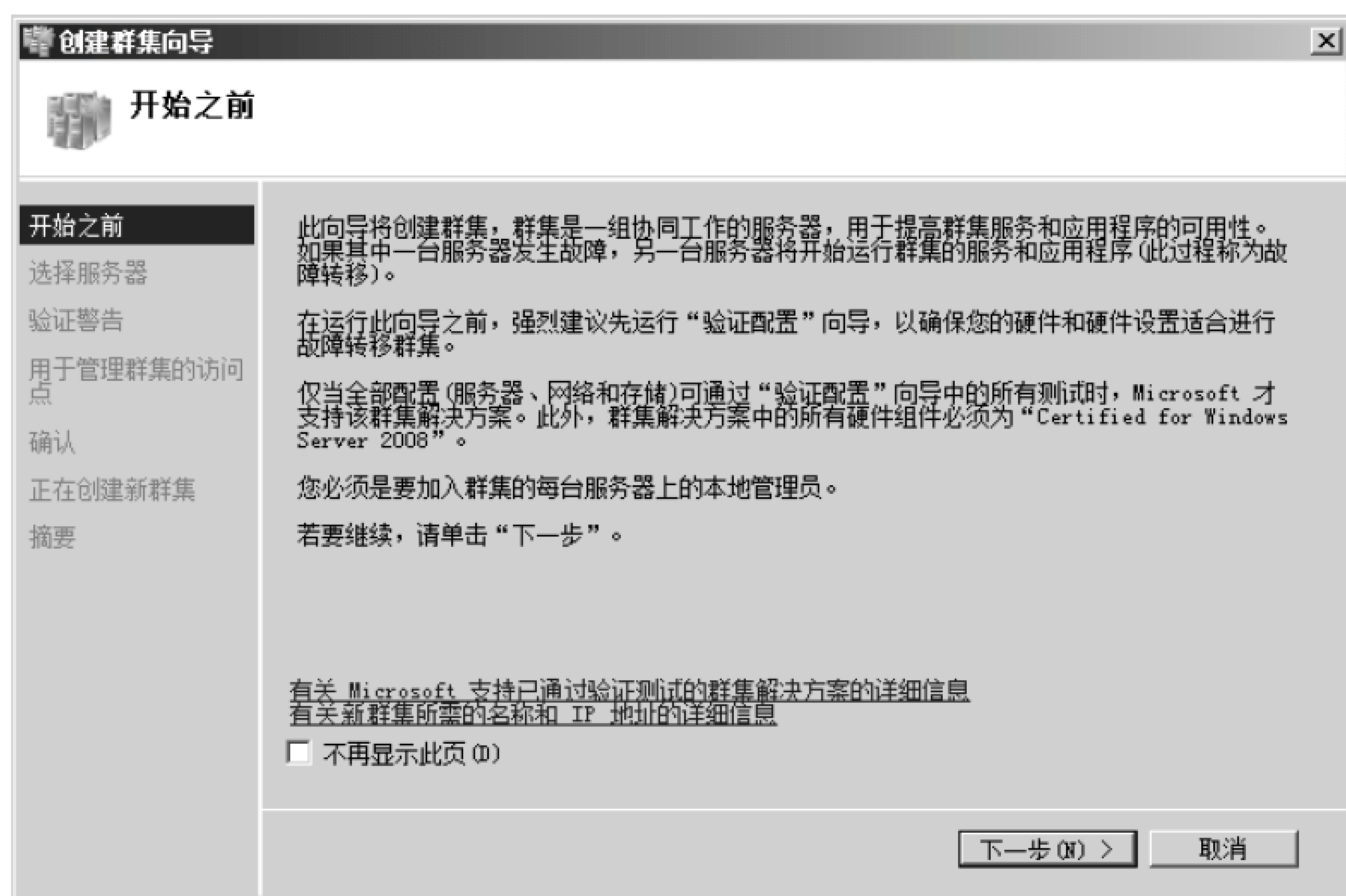


图 14-66 【开始之前】对话框



图 14-67 【选择服务器】对话框

04 弹出【用于管理群集的访问点】对话框，为群集命名，并指定用于管理故障转移群集的节点，单击【下一步】按钮，如图 14-68 所示。

05 弹出【确认】对话框，显示创建群集的配置信息，单击【下一步】按钮，如图 14-69 所示。

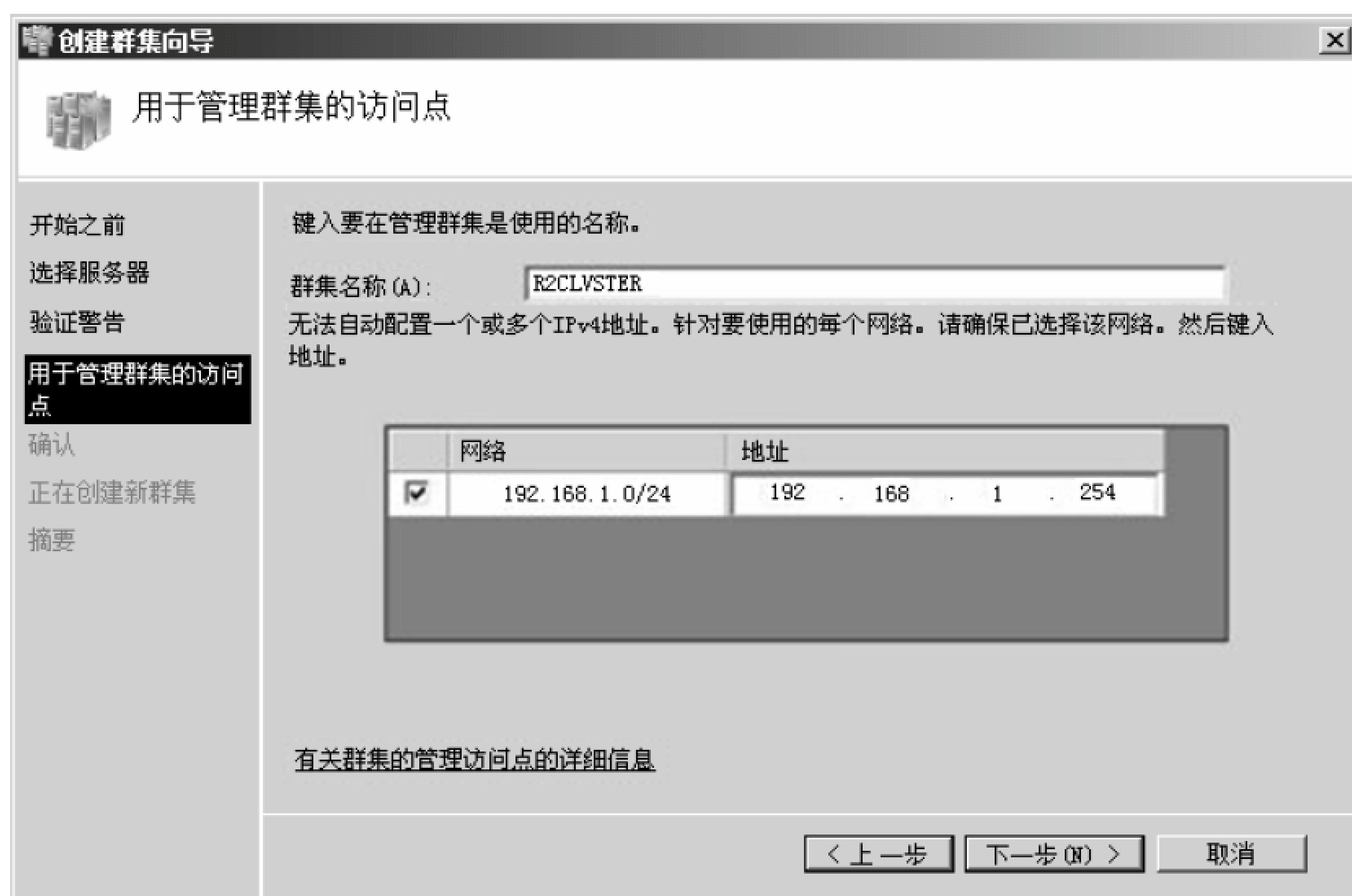


图 14-68 【用于管理群集的访问点】对话框



图 14-69 【确认】对话框

06 弹出【正在创建新群集】对话框，显示创建配置进度，如图 14-70 所示。

07 创建完成后，弹出【摘要】对话框，显示创建信息，单击【完成】按钮结束创建群集过程，如图 14-71 所示。



图 14-70　【正在创建新群集】对话框



图 14-71　【摘要】对话框

群集创建完成后还不能对任何服务和应用提供群集服务，需要使用服务和应用进行添加。

14.4　专家答疑

（1）在群集服务中有群集 IP 地址，是什么意思？群集中的每台计算机都有自己的 IP 地址，为什么还要设置一个群集 IP 地址呢？

答：群集 IP 地址就是整个群集对外服务时的公用 IP 地址，使用群集 IP 地址会让用户访问变得简单，其他主机访问群集只要知道群集 IP，之后会随机连接到一台群集内的服务器，实现分流。

（2）故障转移群集实现时是否需要安装数据库？需要安装什么数据库？

答：做故障转移群集，其主要作用之一就是保障数据的安全可靠，所以一般做故障转移群集都是针对数据库的。所用的数据库没有明确要求，主要取决于企业当前使用的是何种数据库。

第 15 章　网络数据库管理与维护

对于大多数企业，最有价值的并不是路由器、交换机和服务器等硬件设备，而是存在于服务器上的数据。这些数据一般都需要专业的数据库程序进行统一管理及调用，网络管理员需要熟练掌握常规的数据库操作技术。

在行业中专门做数据库系统管理的职业称为数据库管理员（DBA）。DBA 的工作任务主要是安装部署数据库、管理数据库的安全、备份和恢复数据库、监测数据库运行和优化数据库性能等，概括地说，DBA 的任务就是力争确保数据库安全、稳定和高效地运行。

本章将简单介绍市场主流的数据库系统，并以 MySQL 数据库为例，着重介绍其管理与维护方法。

15.1　常见数据库介绍

常见的数据库有三种，MySQL、SQL Server 和 Oracle。三种数据库的内容介绍如下。

1. MySQL 数据库

MySQL 数据库的版本最早是 4.0 版本的，现在大部分用户用的都是 5.0 版本的，本章节以介绍 MySQL 5.0 版本为主。MySQL 数据库是一款开放源代码的关系型数据库管理系统，任何人都可以通过网络免费获得，所以这也使得其在中小企业具有很大的使用比例。同时 MySQL 数据库与近些年比较流行的 PHP 网站开发技术结合较为紧密，由于 PHP 网站开发技术的广泛使用，使得 MySQL 的发展具有非常好的前景。

2. SQL Server 数据库

SQL Server 数据库的版本主要包括 SQL Server 2000 和 SQL Server 2005，最新出版的还有 SQL Server 2008，但是目前 SQL Server 2005 的市场占有率比较高。SQL Server 数据库提供了更安全可靠的存储功能，同时可以满足大型数据服务对高可用性和高性能的要求，适合很多大中型企业。

3. Oracle 数据库

Oracle 数据库包括数据库服务器端和客户端，同时 Oracle 数据库具有支持多用户、大事务量的事务处理，数据安全性和完整性的有效控制，支持分布式数据处理等特性。Oracle 数据库可以按照条件把文本文件数据导入，要比 SQL Server 更稳定、更安全，处理速度方面也比 SQL Server 快

一些，但是 Oracle 数据库价格相对昂贵，并且 Oracle 数据库的易用性和友好性方面比较弱，一般适合对数据要求较高的大型数据库，而且需要配置较高水平的数据库维护人员。

15.2 项目实战 1：MySQL 数据库安装与配置

在 Windows 平台中运行 MySQL 数据库，需要考虑系统是 32 位的还是 64 位的，针对不同的系统选择合适的 MySQL 版本。本节使用 MySQL 5.5 的 32 位版本进行讲解。MySQL 数据库的管理与维护内容介绍如下。

15.2.1 在 Windows 平台下安装与配置 MySQL

Windows 平台下安装 MySQL，可以使用图形化的安装包，图形化的安装包提供了详细的安装向导，通过向导读者可以一步一步完成对 MySQL 的安装，具体操作步骤如下。

01 打开 IE 浏览器，访问网址“http://dev.mysql.com/downloads/mysql/#downloads”，单击【转到】按钮，打开 MySQL Community Server 5.5.13 下载页面，并选择 Generally Available(GA) Release 类型的安装包，下载界面如图 15-1 所示。



图 15-1　MySQL 下载页面

02 在下拉列表框中选择 Microsoft Windows 平台，如图 15-2 所示。



图 15-2　选择 Windows 平台

03 根据读者的平台选择 32 位或者 64 位安装包，在这里选择 32 位，单击右侧 Download 按钮开始下载，如图 15-3 所示。



图 15-3　单击下载 Windows 32 位安装包

04 双击下载的 mysql-5.5.13-win32.msi 文件，如图 15-4 所示。



图 15-4　MySQL 安装文件名称

05 弹出 MySQL 5.5 安装向导对话框，如图 15-5 所示，单击 Next 按钮。

06 打开 End-User License Agreement 对话框，选中 I accept the terms in the License Agreement 复选框，单击 Next 按钮，如图 15-6 所示。



图 15-5　MySQL 5.5 安装向导对话框

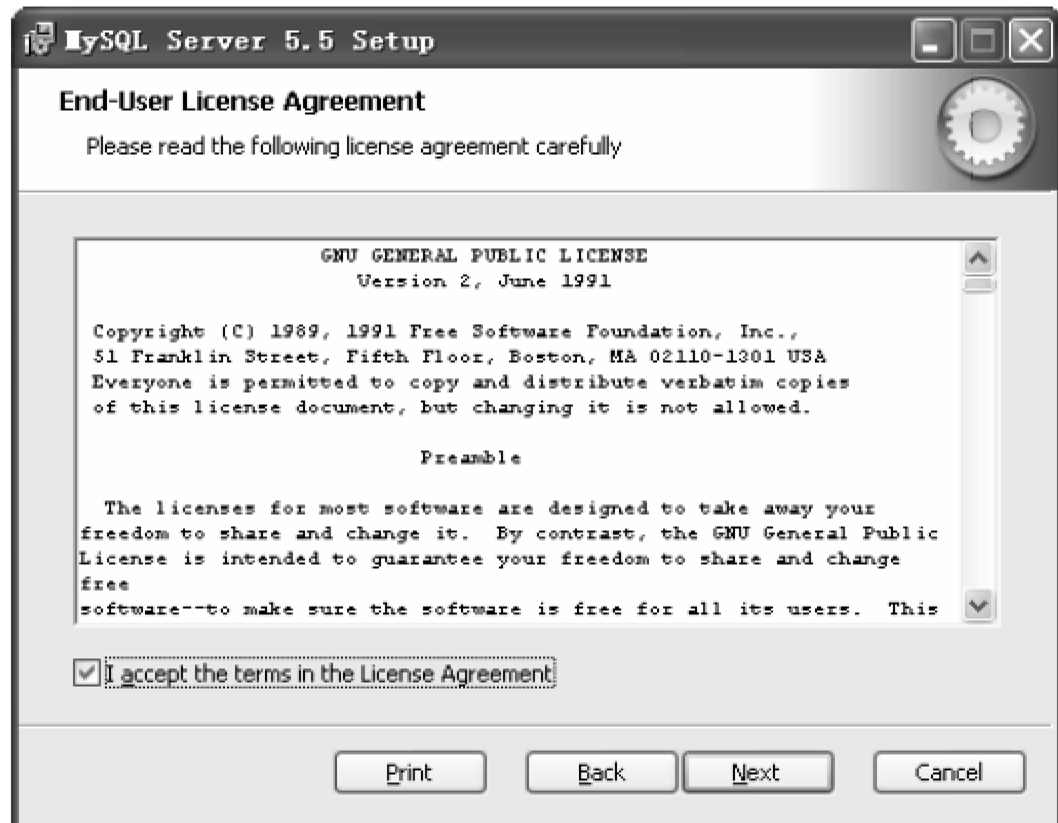


图 15-6　用户许可证协议对话框

07 打开 Choose Setup Type 对话框，在其中列出了 3 种安装类型，分别是 Typical、Custom 和 Complete。如果选择 Typical 或 Complete 这两种安装方式，将进入确认对话框，确认选择并开始安装。如果选择 Custom，将进入 Custom Setup 对话框。在这里选择 Custom，单击 Custom 按钮，如图 15-7 所示。

3 种安装类型的含义如下。

- Typical：安装 MySQL 服务器、MySQL 命令行客户端和命令行实用程序。命令行客户端和

实用程序包括 mysqldump、myisamchk 和其他几个工具来帮助管理 MySQL 服务器。

- Complete: 安装软件包内包含的所有组件。完全安装软件包包括的组件有嵌入式服务器库、基准套件、支持脚本和文档。
- Custom: 安装允许完全控制想要安装的软件包和安装路径。

08 打开 Custom Setup 对话框，如图 15-8 所示。所有可用组件列入 Custom Setup 对话框左侧的树状视图内，未安装的组件用红色 X 图标表示，已经安装的组件有灰色图标。



图 15-7 安装类型对话框

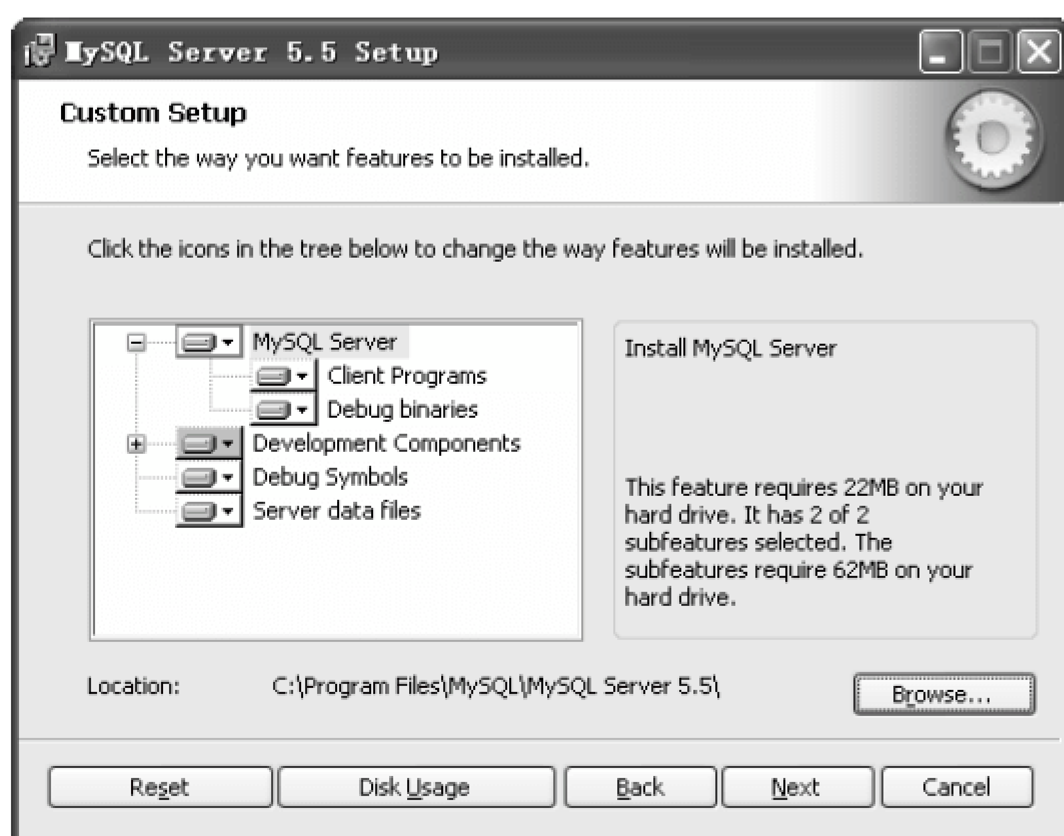


图 15-8 自定义安装组件对话框

09 默认情况下，选择全部安装，要想更改组件，单击该组件的图标并从下拉列表中选择新的选项，并设置安装路径，单击 Next 按钮，如图 15-9 所示。

四个选项的意思分别是：

- Will be installed on local hard drive，表示安装这个附加组件到本地硬盘。
- Entire feature will be installed on local hard drive，表示将安装这个组件特性及其子组件到本地硬盘。
- Feature will be installed when required，表示这个附加组件在需要的时候才安装。
- Entire feature will be unavailable，表示不安装这个组件。



MySQL 默认安装路径为“C:\Program Files\MySQL\MYSQL\MySQL Server 5.5\”可以单击安装路径右侧的 Browse 按钮来更改默认安装路径。

10 进入安装确认对话框，单击 Install 按钮，如图 15-10 所示。

11 开始安装 MySQL 文件，安装向导过程中所做得设置将在安装完成之后生效，用户可以通过进度条看到当前安装进度，如图 15-11 所示。

12 安装完成后，将弹出有关 MySQL Enterprise 版的介绍说明对话框，单击【More】按钮，如图 15-12 所示。

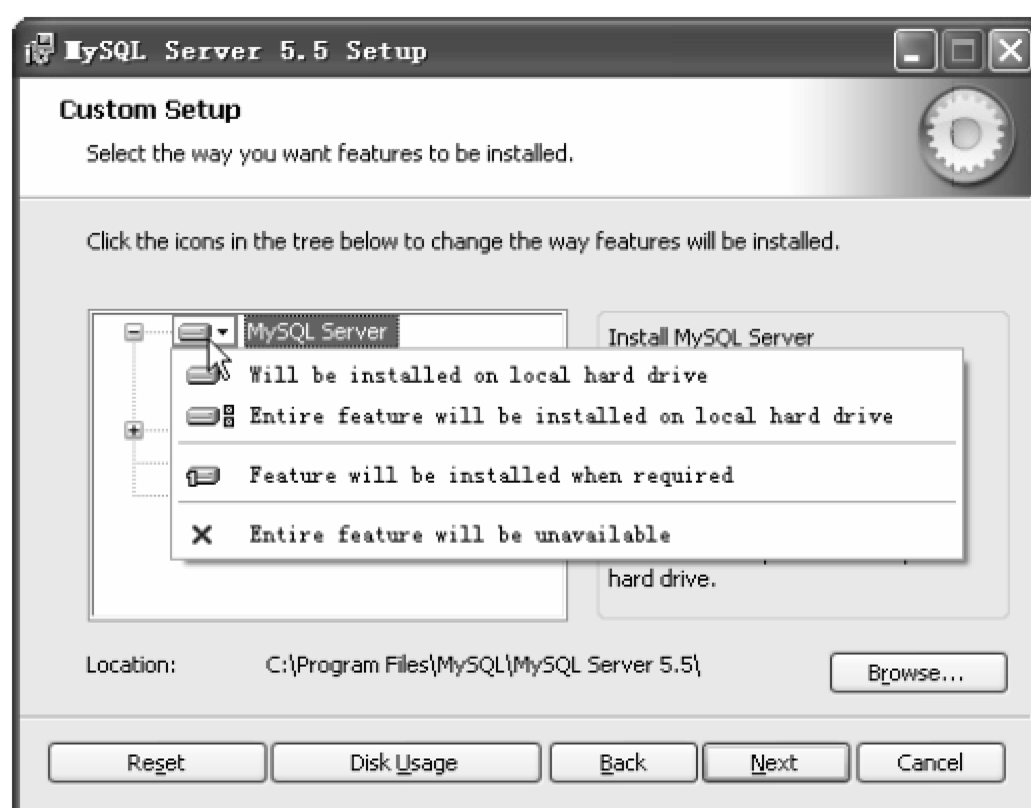


图 15-9　更改组件菜单

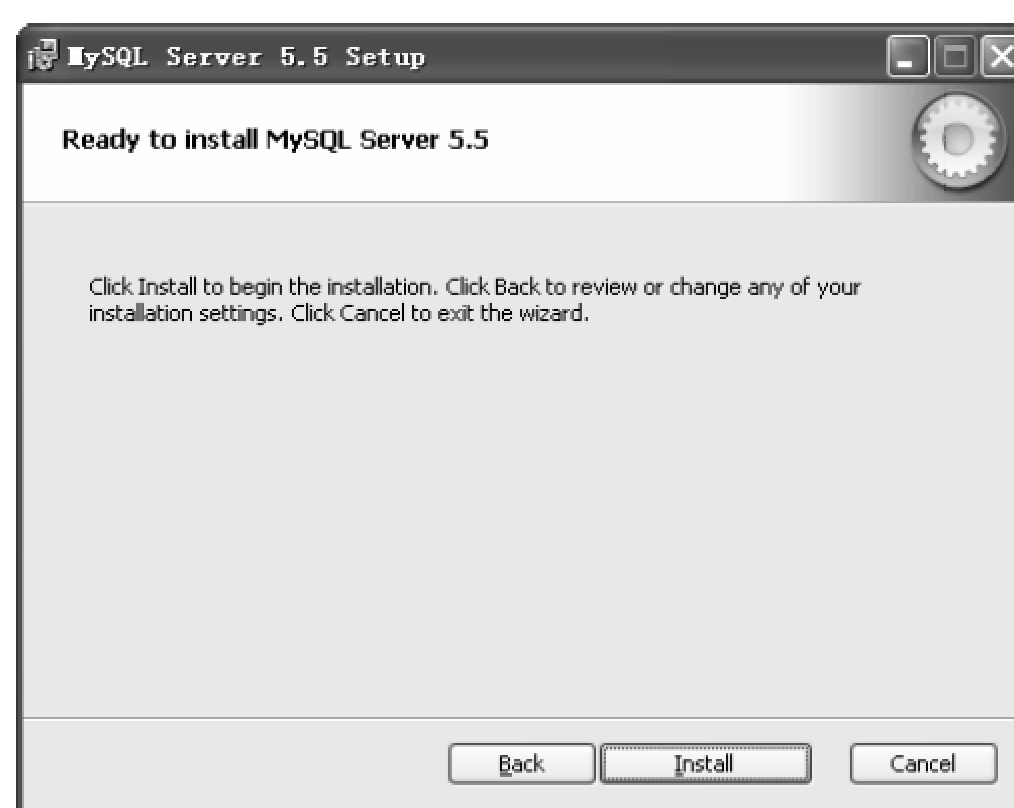


图 15-10　准备安装对话框

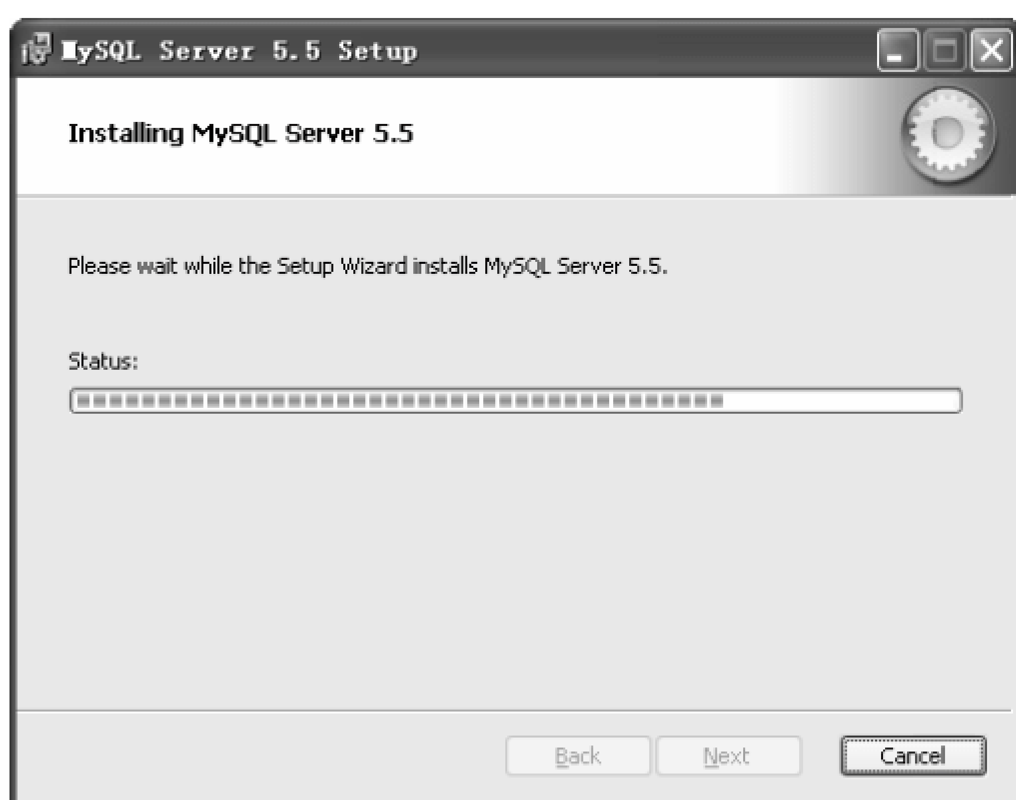


图 15-11　安装进度对话框

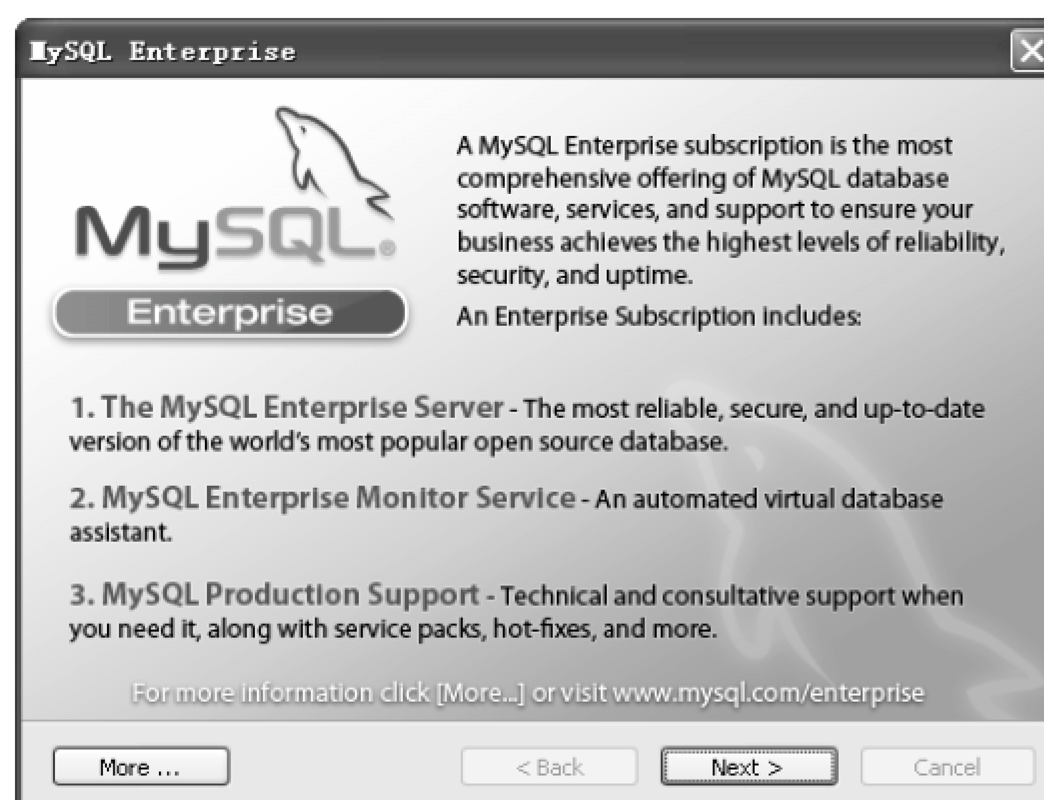


图 15-12　介绍对话框

13 在浏览器中打开一个页面，单击 Next 按钮进入第二个介绍对话框，如图 15-13 所示。

14 单击 Next 按钮，进入安装完成界面，如图 15-14 所示。

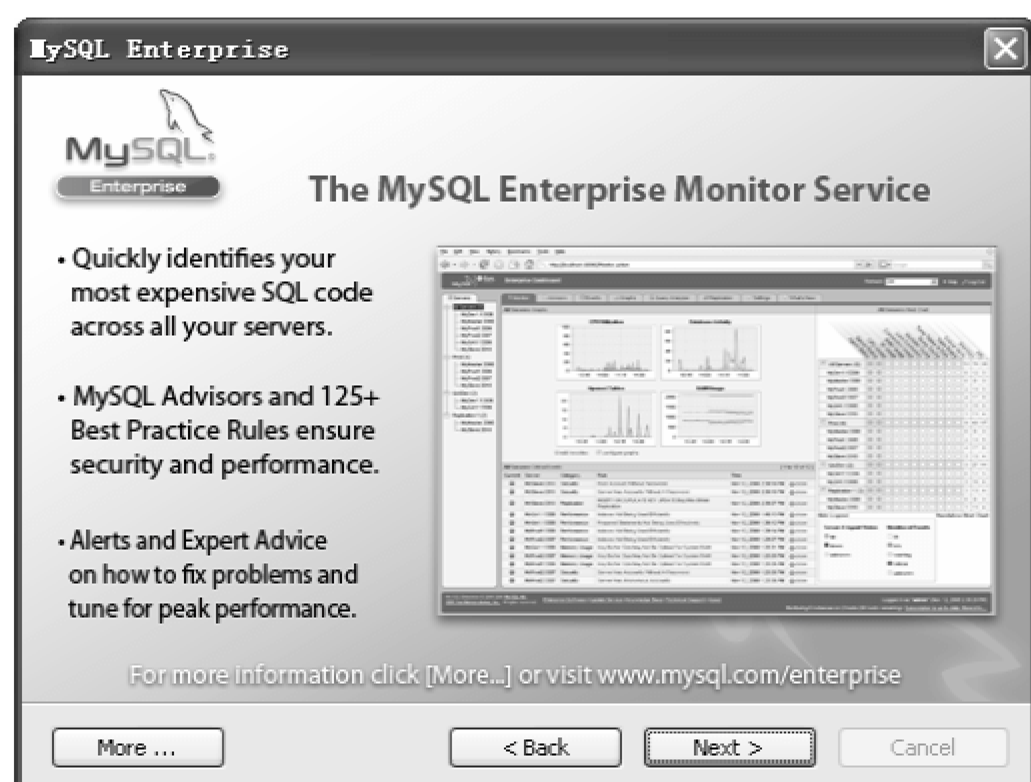


图 15-13　介绍对话框

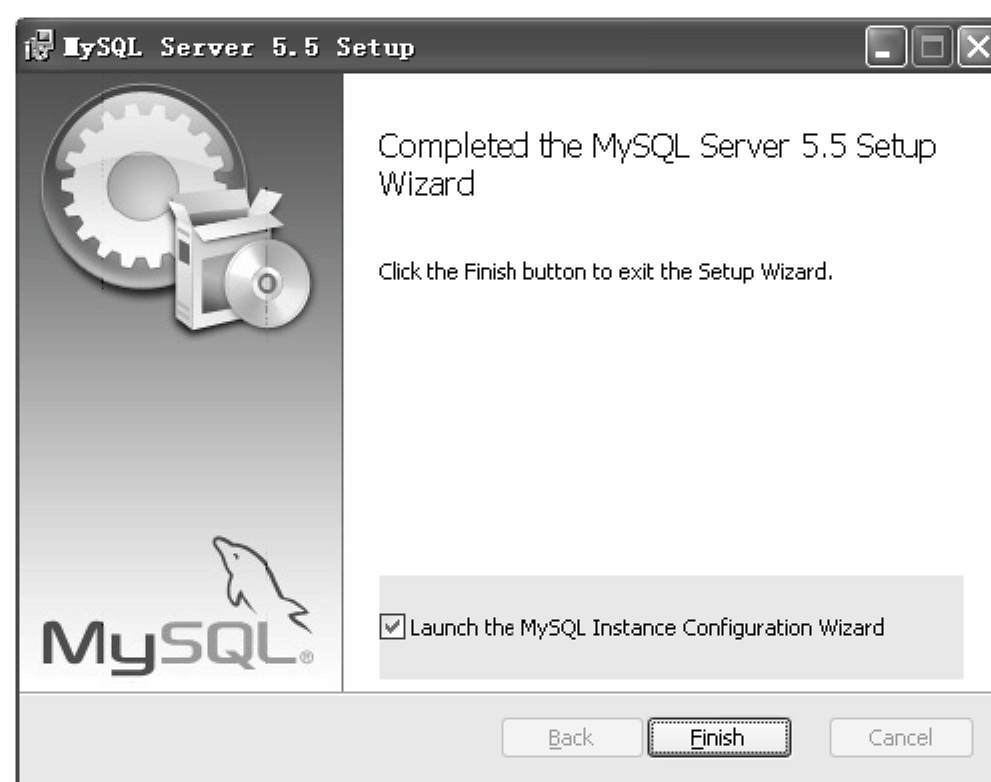


图 15-14　安装完毕介绍对话框



在安装完成对话框有一个选项【Launch the MySQL Instance Configuration Wizard】，选择该选项，MySQL 安装文件将启动 MySQL 配置向导。此处，选中选项，然后单击 Finish 按钮，将进入 MySQL 配置向导对话框，开始配置 MySQL。如果此处取消选中该选项，还可以进入 MySQL 安装 bin 目录直接启动 MySQLInstanceConfig.exe 文件，进行配置 MySQL。

15.2.2 配置 MySQL 5.5

MySQL 安装完毕之后，需要对服务器进行配置，使用图形化的配置工具 MySQLInstanceConfig.exe。启动 MySQL Instance Configuration Wizard，或者在 MySQL 安装目录下的 bin 目录中直接双击 MySQLInstanceConfig.exe 启动配置向导。具体的配置步骤介绍如下。

01 启动配置向导，进入配置对话框，如图 15-15 所示。

02 单击 Next 按钮，进入选择配置类型对话框，在配置类型对话框中可以选择两种配置类型：Detailed Configuration 和 Standard Configuration，如图 15-16 所示。

各选项含义介绍如下：

- Standard Configuration：该选项适合想要快速启动 MySQL 而不必考虑服务器配置的新用户。
- Detailed Configuration：该选项适合想要更加详细地控制服务器配置的高级用户。

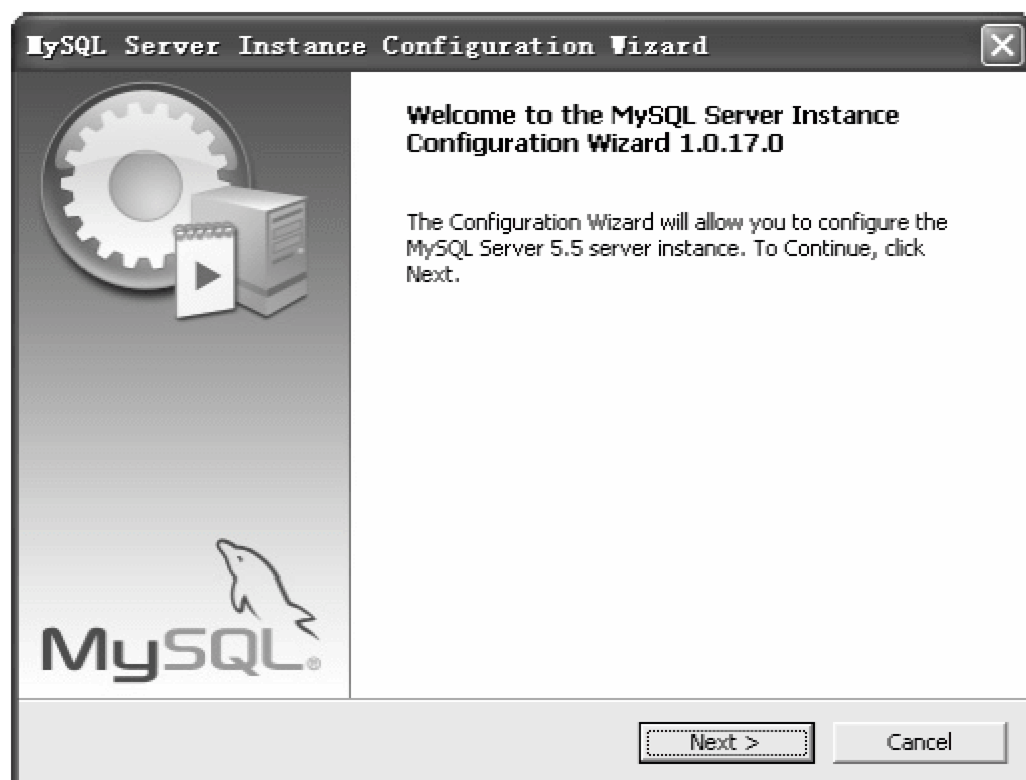


图 15-15 配置向导介绍对话框

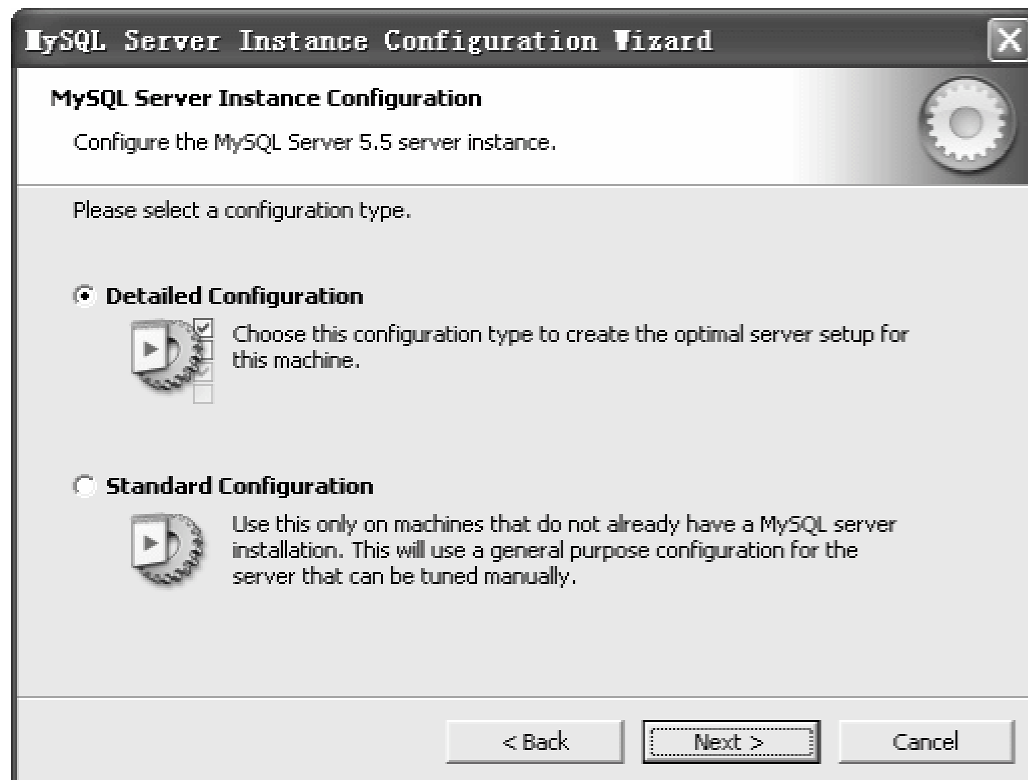


图 15-16 配置类型介绍对话框

03 为了学习 MySQL 的配置过程，在此选择详细配置选项，单击 Next 按钮，进入服务器类型对话框，可以选择 3 种服务器类型，选择哪种服务器将影响到 MySQL Configuration Wizard 对内存、硬盘和过程或使用的决策，如图 15-17 所示。作为初学者，选择 Developer Machine 已经足够了，这样占用系统的资源不会很多。

各选项含义介绍如下。

- Developer Machine：该选项代表典型个人用桌面工作站。假定机器上运行着多个桌面应用程序。将 MySQL 服务器配置成使用最少的系统资源。
- Server Machine：该选项代表服务器，MySQL 服务器可以同其他应用程序一起运行，如 FTP、

E-mail 和 Web 服务器。MySQL 服务器配置成使用适当比例的系统资源。

- Dedicated MySQL Server Machine：该选项代表只运行 MySQL 服务的服务器。假定没有运行其他应用程序，MySQL 服务器配置成使用所有可用系统资源。

04 单击 Next 按钮，进入选择数据库用途对话框，在该对话框有 3 个选项，一般选择第一个单选按钮，即多功能数据库，如图 15-18 所示。

各选项含义介绍如下。

- Multifunctional Database：选择该选项，则同时使用 InnoDB 和 MyISAM 储存引擎，并在两个引擎之间平均分配资源。建议经常使用两个储存引擎的用户选择该选项。
- Transactional Database Only：该选项同时使用 InnoDB 和 MyISAM 储存引擎，但是将大多数服务器资源指派给 InnoDB 储存引擎。建议主要使用 InnoDB，偶尔使用 MyISAM 的用户选择该选项。
- Non-Transactional Database Only：该选项完全禁用 InnoDB 储存引擎，将所有服务器资源指派给 MyISAM 储存引擎。仅支持不支持事务的 MyISAM 数据类型。



图 15-17　服务器类型介绍对话框

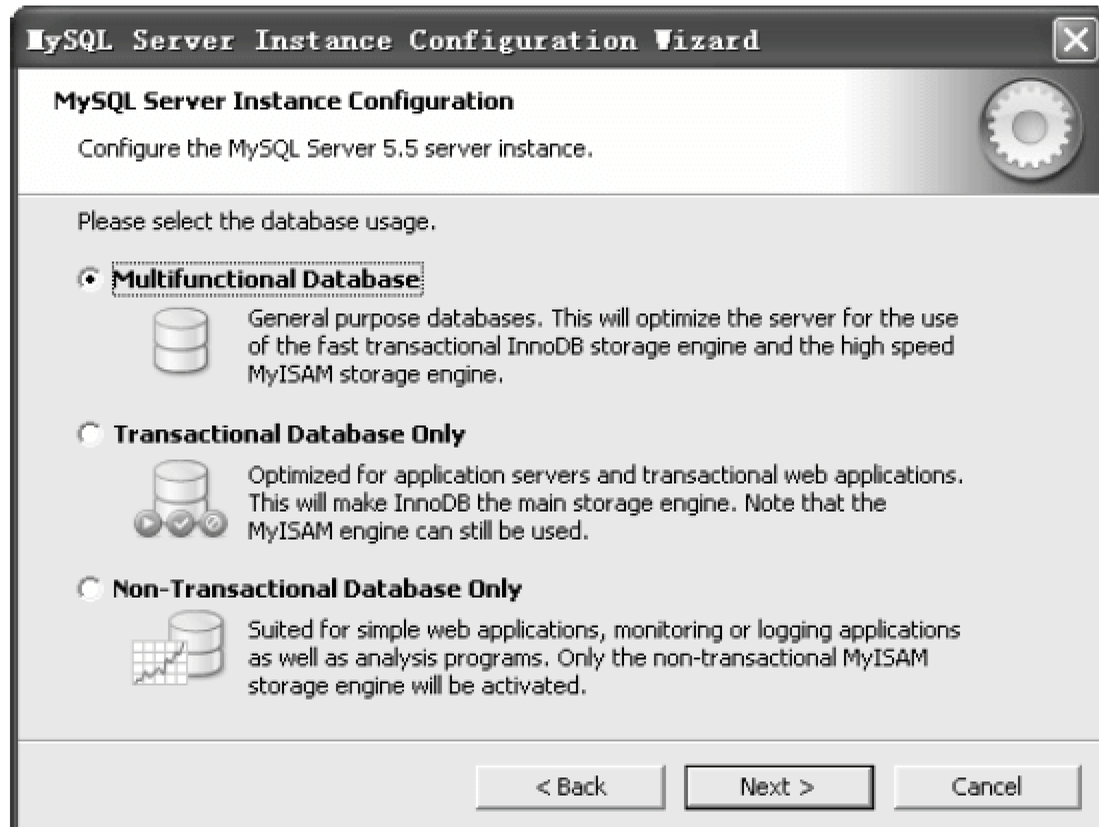


图 15-18　数据库用途对话框

05 单击 Next 按钮，进入 InnoDB 表空间配置对话框中，如图 15-19 所示，为 InnoDB 数据库文件选择存储位置，一般可以直接选择默认，Drive Info 显示了存放位置的分区信息。

06 单击 Next 按钮，进入设置服务器最大并发连接数对话框中，该对话框提供了 3 种不同的连接选项，读者可以根据自己的需要选择，在这里选择默认选项 15，如图 15-20 所示。

各选项含义介绍如下。

- Decision Support（DSS）/OLAP：决策支持。如果服务器不需要大量的并行连接可以选择该选项。假定最大连接数目设置为 100，平均并行连接数为 20。
- Online Transaction Processing（OLTP）：联机事务处理。如果服务器需要大量的并行连接则选择该选项。最大连接数设置为 500。

- Manual Setting：人工设置。选择该选项可以手动设置服务器并行连接的最大数目。从下拉列表框中选择并行连接的数目，如果期望的数目不在列表中，则在下拉列表框中输入最大连接数。

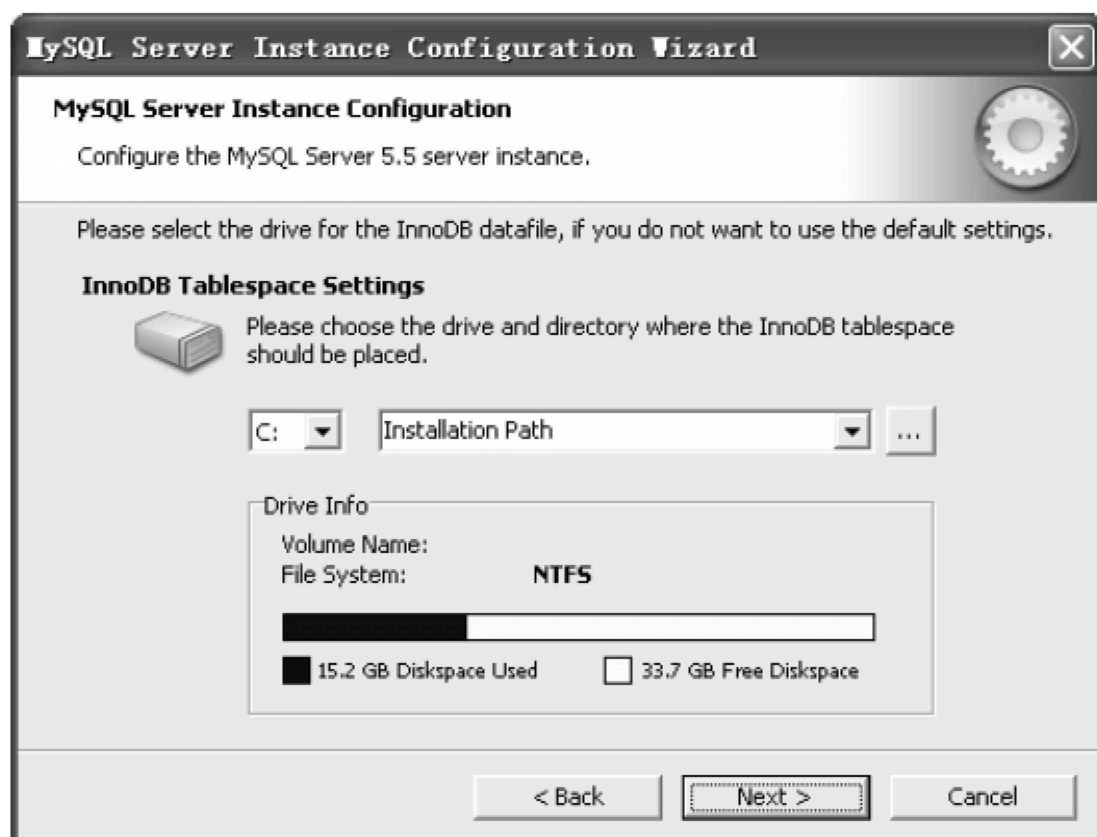


图 15-19　InnoDB 表空间设置对话框

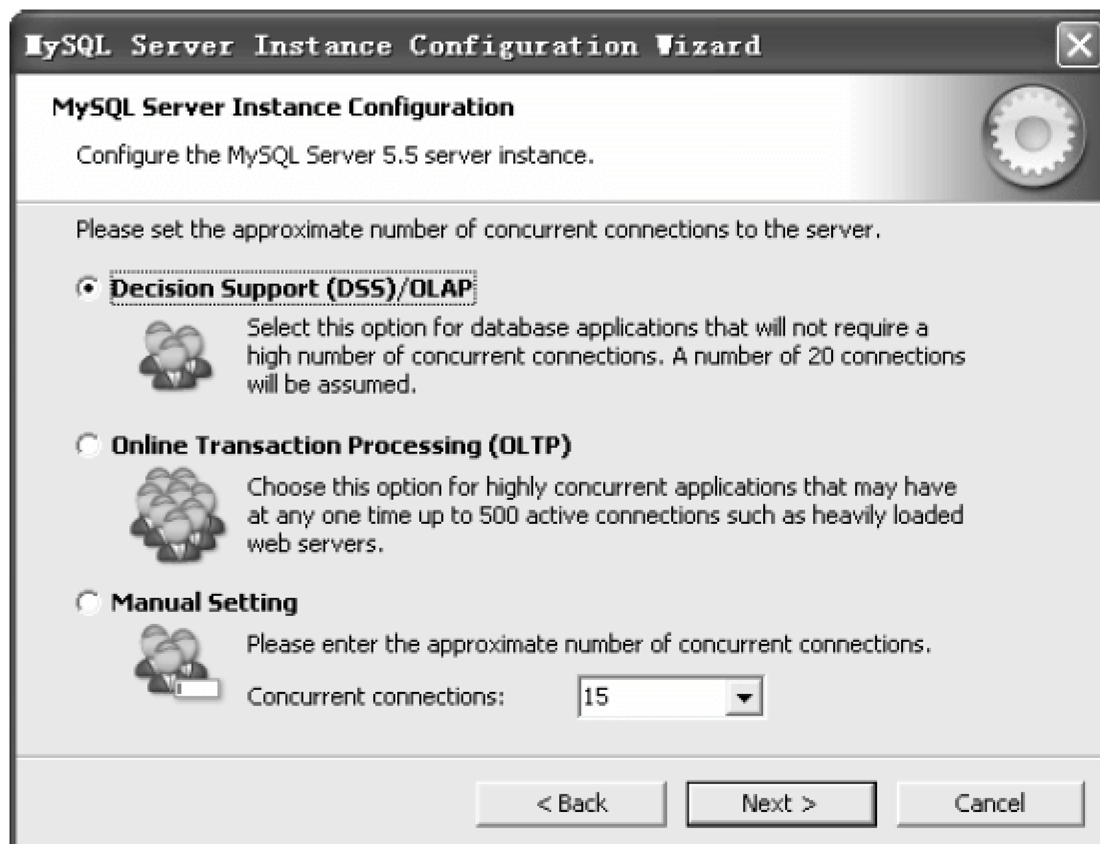


图 15-20　并发连接数设置对话框

07 单击 Next 按钮，进入设置网络选项对话框中，在 Networking Options 对话框中可以启用或禁用 TCP/IP 网络，并配置用来连接 MySQL 服务器的端口号，默认情况启用 TCP/IP 网络，默认端口为 3306。要想更改访问 MySQL 使用的端口，从下拉列表框中选择一个新端口号或直接向下拉列表框中输入新的端口号，但要保证选择的端口号没有被占用。如果选择 Add firewall exception for this port 复选框，防火墙将允许通过该端口访问，在这里选中该选项。如果选中 Enable Strict Mode 选项，MySQL 会对输入的数据进行严格的检验，对于初学者来说，可以不用选择，在这里取消该选项，如图 15-21 所示。

08 单击 Next 按钮，打开用于设置 MySQL 默认语言编码字符集的对话框，该对话框提供了 3 种类型字符集，如果要支持中文，常用的选项有 latin1、gb2312、gbk 或者 utf-8，如果都是英文字符，可以选择 latin1，如果要支持中文可以选择国标 gb2312 或者 gbk，如果要支持多国语言可以选择 utf-8，在这里选择 utf-8，从第三个选项的下拉列表中选择 utf-8，如图 15-22 所示。

各选项含义介绍如下。

- Standard Character Set：标准字符集。如果想要使用 Latin1 作为默认服务器字符集，则选择该选项。Latin1 用于英语和许多西欧语言。
- Best Support For Multilingualism：支持多种语言。如果想要使用 UTF8 作为默认服务器字符集，则选择该选项。UTF8 可以将不同语言的字符储存为单一的字符集。
- Manual Selected Default Character Set/Collation：人工选择的默认字符集/校对规则。如果想要手动选择服务器的默认字符集，请选择该项。从下拉列表中选择期望的字符集。

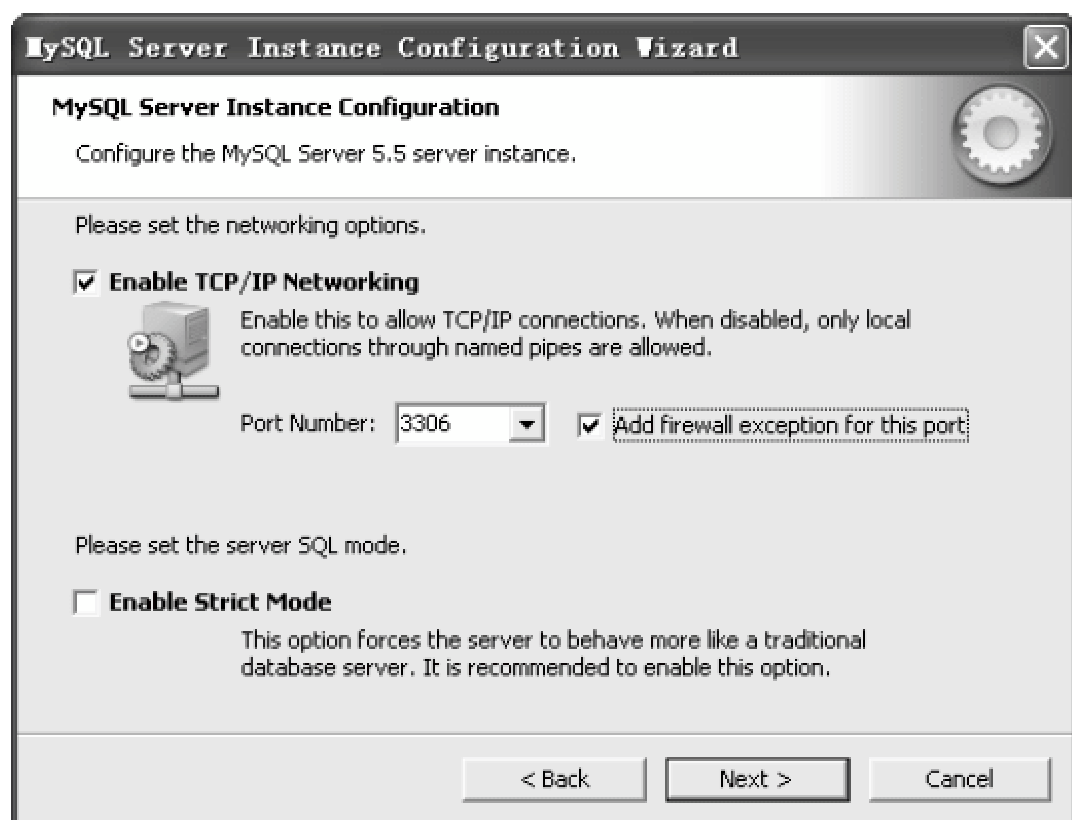


图 15-21　网络选项设置对话框

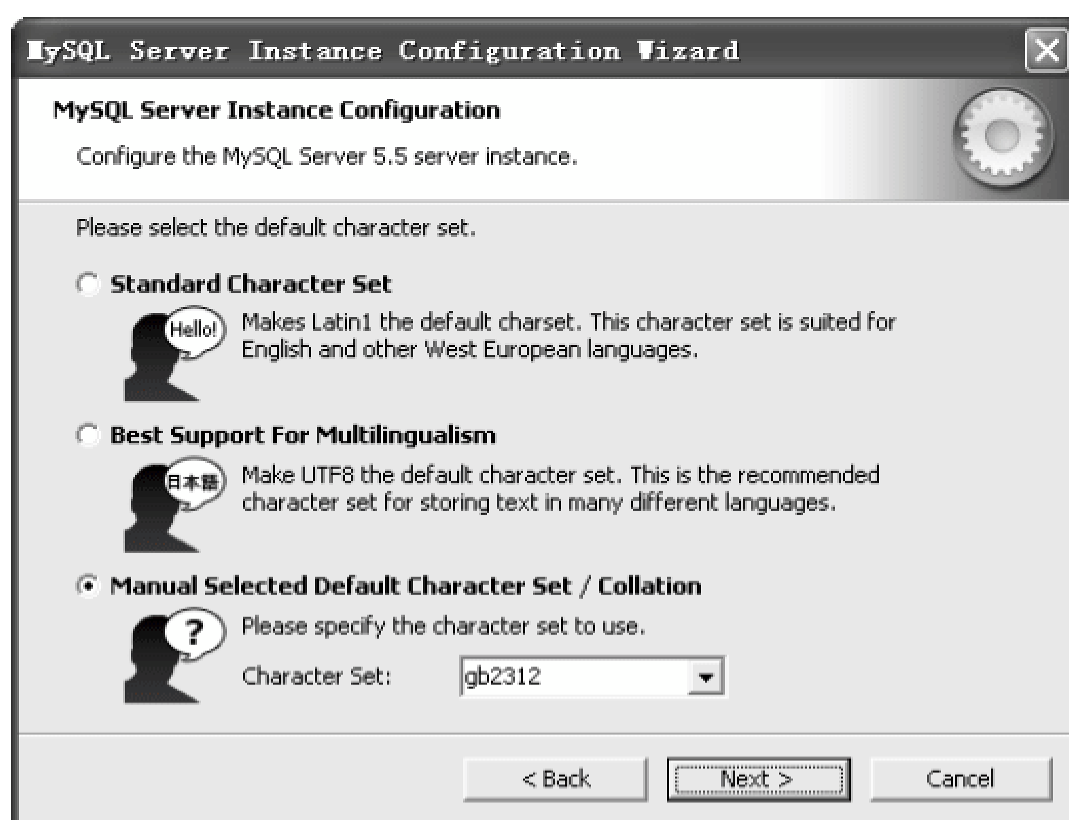


图 15-22　默认字符集设置对话框

09 单击 Next 按钮，进入用于设置 Windows 选项的对话框，如图 15-23 所示。这一步选择将 MySQL 安装为 Windows 服务，并制定服务名称。

各选项含义介绍如下。

- 选中 Install As Windows Service 复选框将 MySQL 安装为 Windows 服务。
- 在 Service Name 右边的下拉列表框中可以选择服务名称，也可以自己输入。
- 选中 Launch the MySQL Server automatically 选项，则 Windows 启动之后 MySQL 会自动启动。
- 选中 Include Bin Directory in Windows PATH 选项，MySQL 的 bin 目录将会添加到环境变量 PATH 中，这样以后在 cmd 模式下，可以直接使用 bin 目录下的文件，而不用每次都输入完整的地址。

10 单击 Next 按钮，进入用于设置安全选项的对话框，如图 15-24 所示。

各选项含义介绍如下。

- 要想设置 root 密码，在 New root password 和 Confirm 两个文本框内输入期望的密码。
- 要想禁止通过网络以 root 登录，不用选中 Enable root access from remote machines（只允许从本机登录连接 root）复选框。这样可以提高 root 账户的安全。
- 要想创建一个匿名用户账户，选中 Create An Anonymous Account（创建匿名账户）复选框。创建匿名账户会降低服务器的安全，因此不建议选中该选项。
- 如果不想设置 root 密码，不选中 Modify Security Settings（修改安全设定值）复选框。

11 单击 Next 按钮，进入准备执行配置对话框。如图 15-25 所示。

12 如果对设置确认无误，单击 Execute 按钮，MySQL Server 配置向导执行一系列的任务，并在对话框中显示任务进度，执行完毕之后显示如图 15-26 所示。单击 Finish 按钮完成整个配置过程。

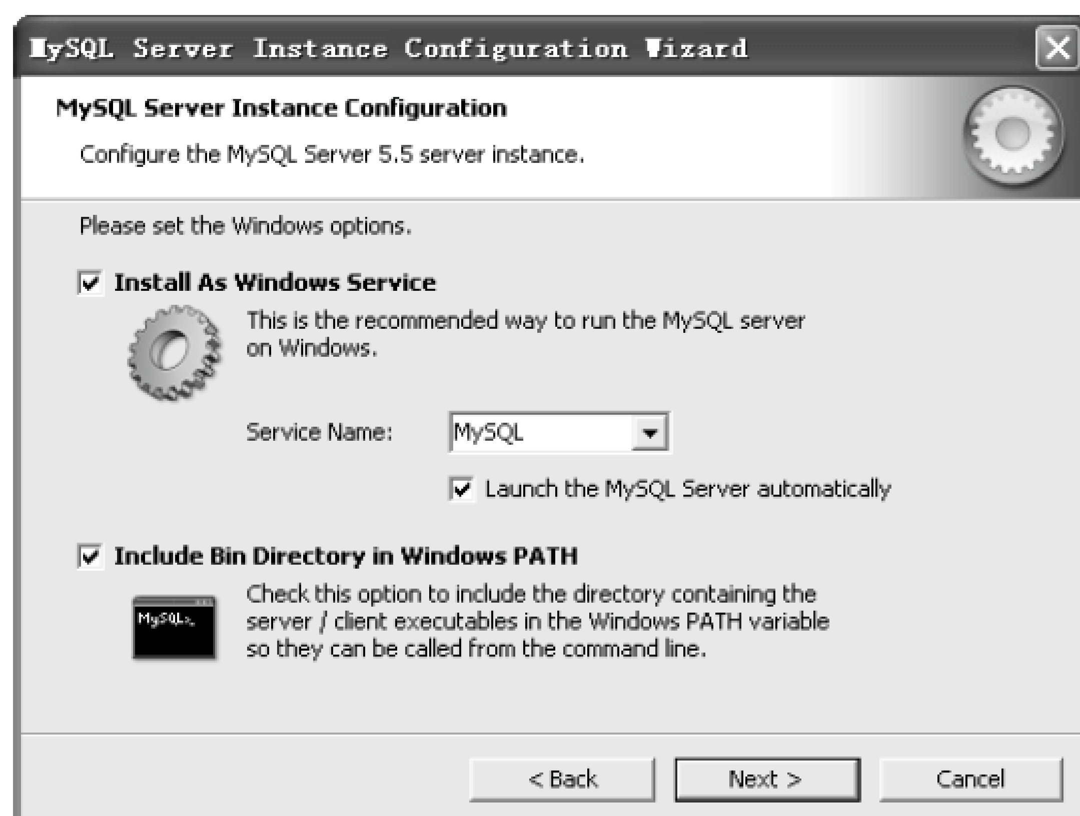


图 15-23　Windows 选项设置对话框



图 15-24　安全设置对话框

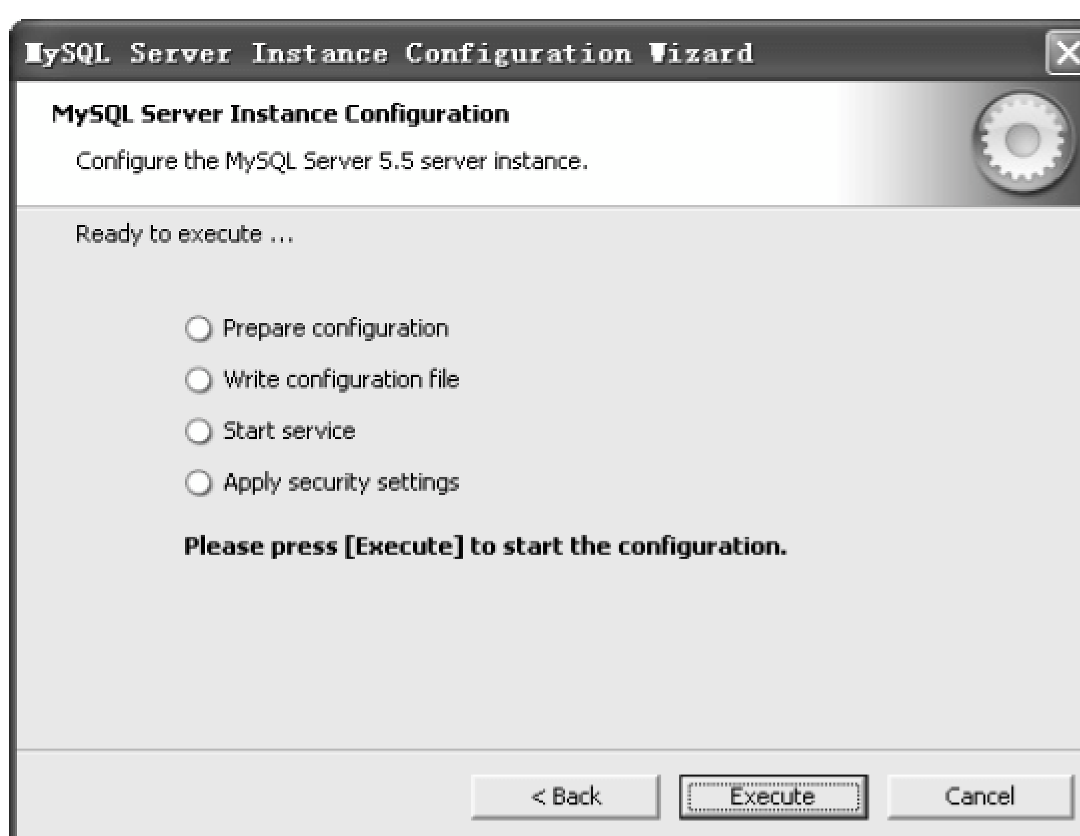


图 15-25　准备执行配置对话框

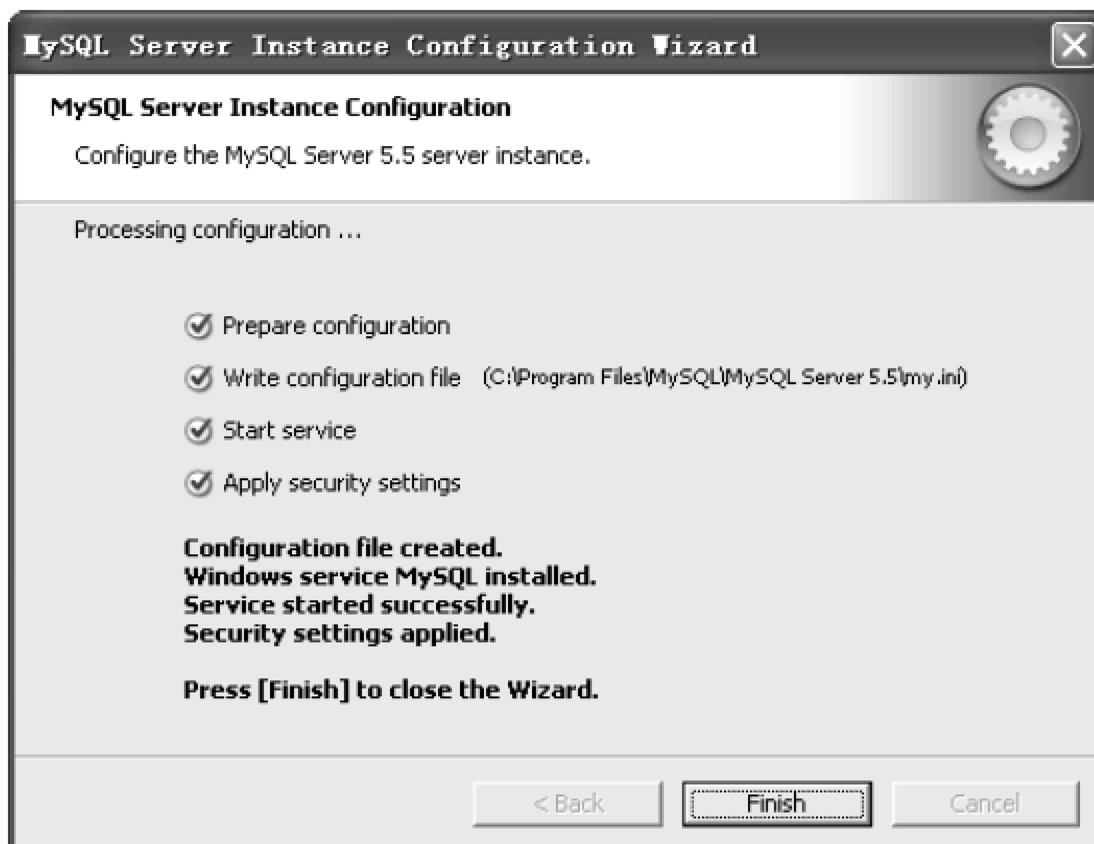


图 15-26　配置完毕对话框

13 按 Ctrl+Alt+Del 组合键，打开【Windows 任务管理器】对话框，可以看到 MySQL 服务进程 mysqld.exe 已经启动了，如图 15-27 所示。至此，就完成了在 Windows XP 操作系统环境下安装 MySQL 的操作。



图 15-27　任务管理器窗口

15.3 项目实战 2：MySQL 数据库的启用与管理

MySQL 安装完毕之后，需要启动服务器进程，并完成基本环境配置才可以使用 MySQL 数据库。数据库搭建完成后，数据库管理员需要掌握基本的数据库创建与删除方法。

15.3.1 启用 MySQL

安装完成后，想要使用 MySQL 数据库，还需要经历三个步骤，介绍如下。

1. 启动 MySQL 服务

在前面的配置过程中，已经将 MySQL 安装为 Windows 服务，当 Windows 启动、停止时，MySQL 也自动启动、停止。不过，用户还可以使用图形服务工具来控制 MySQL 服务器或从命令行使用 net 命令。

可以通过 Windows 的服务管理器查看。具体的操作步骤如下。

01 单击【开始】菜单，在弹出的菜单中选择【运行】命令，打开【运行】对话框，在【打开】文本框中输入“services.msc” ，单击【确定】按钮，如图 15-28 所示。



图 15-28 【运行】对话框

02 打开 Windows 的【服务管理器】，在其中可以看见服务名为“MySQL”的服务项，其右边状态“已启动”表明该服务已启动，如图 15-31 所示。

名称	描述	状态	启动类型	登录为
MySQL		已启动	自动	本地系统
MS Software Sh...	管...		手动	本地系统
Messenger	传...		已禁用	本地系统
Logical Disk M...	配...		手动	本地系统

图 15-29 服务管理器窗口

由于设置了 MySQL 为自动启动，在这里可以看到，服务已经启动，而且启动类型为自动。如果没有“已启动”字样，说明 MySQL 服务未启动。启动方法为：单击【开始】菜单，选择【运行】命令，在【运行】对话框中输入“cmd”，按 Enter 键弹出 XP 命令提示符界面。然后输入“net start mysql”，按 Enter 键，就能启动 mysql 服务了；停止 mysql 服务的命令为“net stop mysql”，如图 15-30 所示。



图 15-30　命令行中启动和停止 MySQL



提示　输入的 MySQL 是服务的名字。如果读者的 MySQL 服务的名字是 DB 或其他名字，应该输入“net start DB”或其他名。

也可以直接双击 MySQL 服务，打开【MySQL 属性】对话框，在其中通过单击【启动】或【停止】按钮来更改服务状态，如图 15-31 所示。



图 15-31　MySQL 服务属性对话框

2. 登录 MySQL 数据库

当 MySQL 服务启动完成后，便可以通过客户端来登录 MySQL 数据库。在 Windows 操作系统下，可以通过两种方式登录 MySQL 数据库。

1）以 Windows 命令行方式登录

具体的操作步骤如下。

01 单击【开始】菜单，在弹出的菜单中选择【运行】命令，打开【运行】对话框，在其中输入命令“cmd”，如图 15-32 所示。

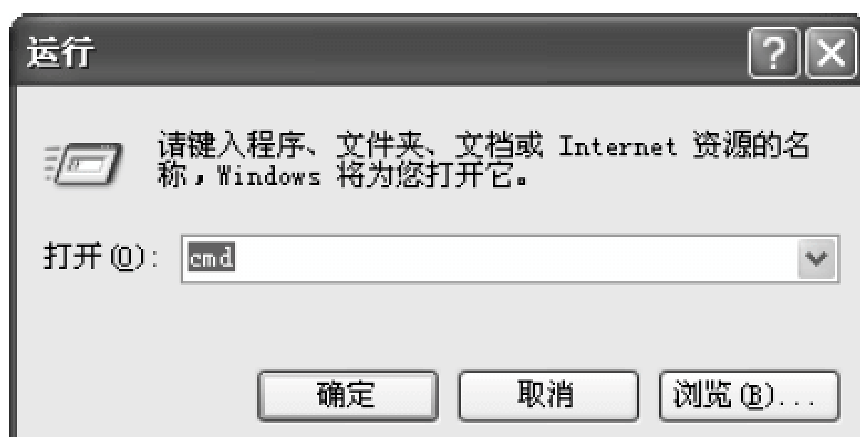


图 15-32　【运行】对话框

02 单击【确定】按钮，打开 DOS 窗口，如图 15-33 所示。



图 15-33　DOS 窗口

03 在 DOS 窗口中可以通过登录命令连接到 MySQL 数据库，连接 MySQL 的命令格式为:

```
mysql -h hostname -u username -p
```

其中 mysql 为登录命令，–h 后面的参数是服务器的主机地址，在这里客户端和服务器在同一台机器上，所以输入 localhost 或者 IP 地址 127.0.0.1，-u 后面跟登录数据库的用户名称，在这里为 root，-p 后面是用户登录密码。

在这里，输入命令如下：

```
mysql   -h localhost –u root –p
```

按 Enter 键，系统会提示输入密码“Enter password”，这里输入在前面配置向导中自己设置的密码，验证正确后，即可登录到 MySQL 数据库，如图 15-34 所示。

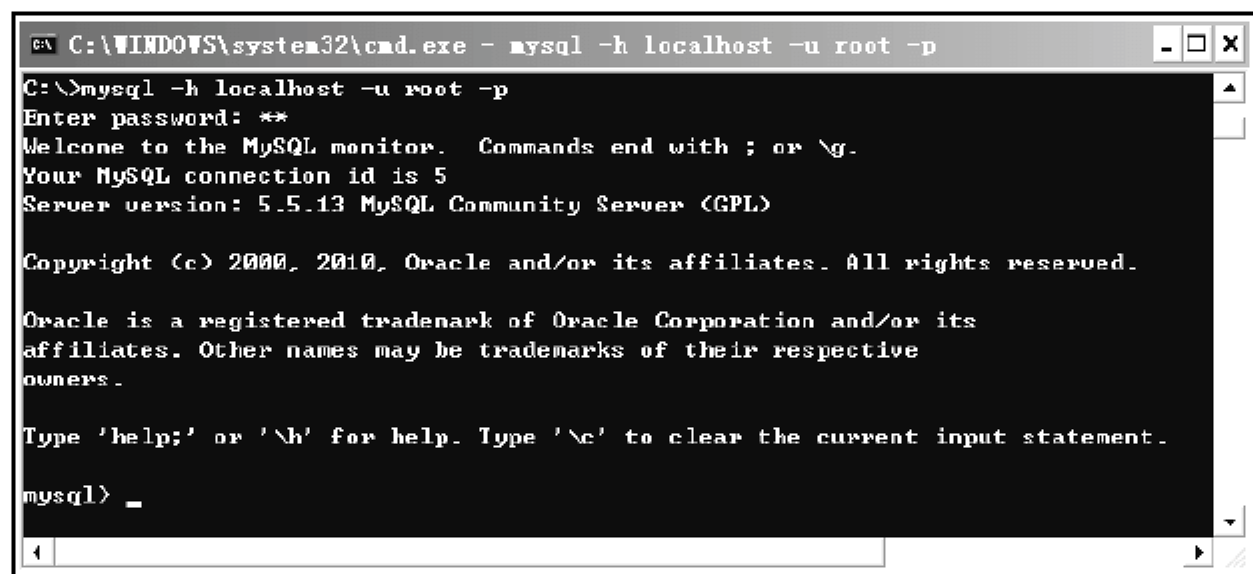


图 15-34　Windows 命令行登录窗口



提　示

当窗口中出现这些说明信息，命令提示符变为“mysql>”时，说明已经成功登录 MySQL 服务器了，可以开始对数据库进行操作。

2）使用 MySQL Command Client Line 登录

依次选择【开始】➢【所有程序】➢【MySQL】➢【MySQL Server 5.5】➢【MySQL 5.5 Command Client Line】命令，进入密码输入窗口，如图 15-35 所示。

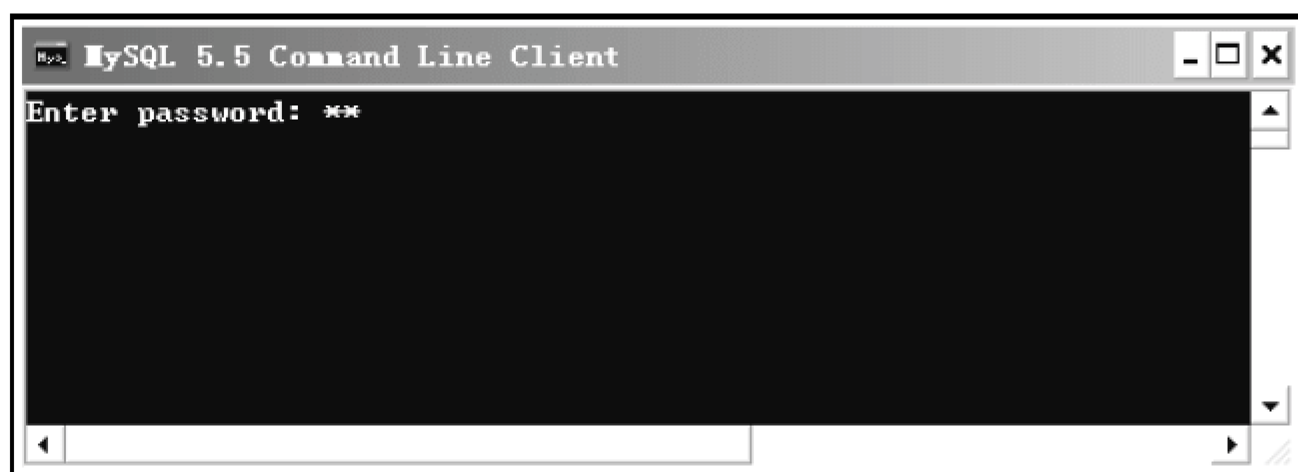


图 15-35　MySQL 命令行登录窗口

输入正确的密码之后，就可以登录到 MySQL 数据库了。

此外，还有一种是通过 MySQL 图形化管理工具登录数据库的方式，这里暂不介绍，有兴趣的读者，可以查阅相关资料，学习这些图形化工具的使用。

3. 配置 Path 变量

在前面登录 MySQL 服务器的时候，直接输入 mysql 登录命令，因为把 MySQL 的 bin 目录添加到了系统的环境变量里面，所以可以直接这样使用。

如图 15-23 所示，选中 Include Bin Directory in Windows PATH 复选框，MySQL 的 bin 目录将会添加到环境变量 PATH 中。如果没有把 MySQL 的 bin 目录添加到系统的变量 PATH 中，那么每次在命令行下都要输入完整的 bin 目录路径或者切换到 bin 目录，例如“cd C:\Program Files\MySQL\MySQL Server 5.5\bin”，才能使用 mysql 等其他命令工具，这样比较麻烦。

下面介绍怎样手动配置 Path 变量，具体的操作步骤如下。

01 在桌面上右击【我的电脑】图标，在弹出的快捷菜单中选择【属性】命令，如图 15-36 所示。

02 打开【系统属性】对话框，并选择【高级】选项卡，如图 15-37 所示。



图 15-36　【我的电脑】属性菜单

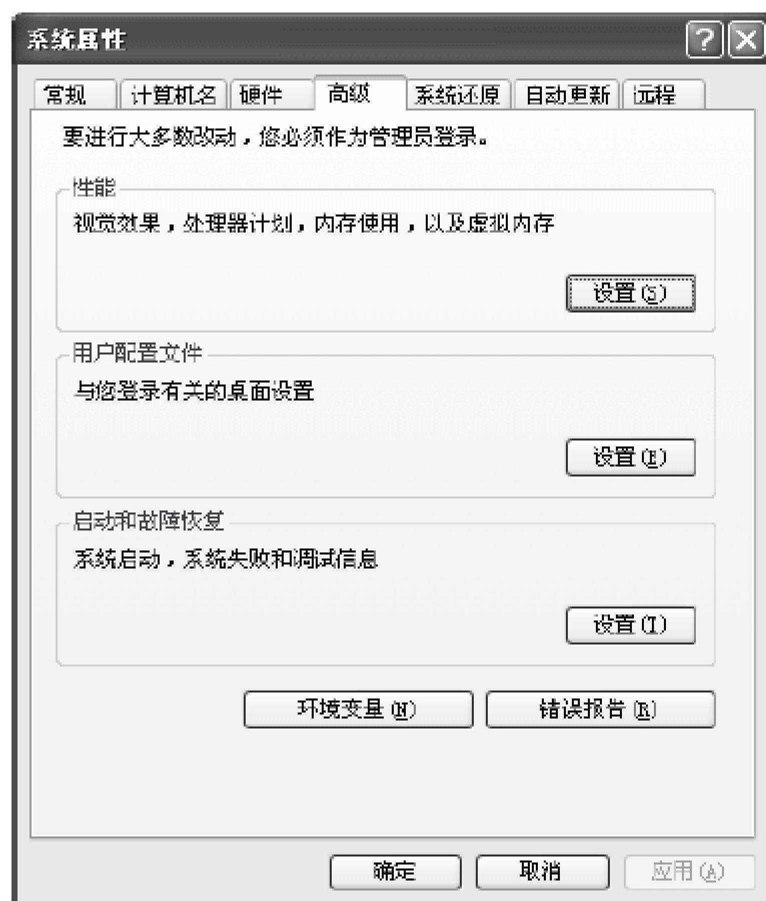


图 15-37　【系统属性】对话框

03 单击【环境变量】按钮，打开【环境变量】对话框，在【系统变量】列表框中选择 Path 变量，如图 15-38 所示。

04 单击【编辑】按钮，打开【编辑系统变量】对话框中，将 MySQL 应用程序的 bin 目录 C:\Program Files\MySQL\MySQL Server 5.5\bin 添加到变量值中，用分号将其与其他路径分隔开，如图 15-39 所示。



图 15-38　【系统变量】对话框

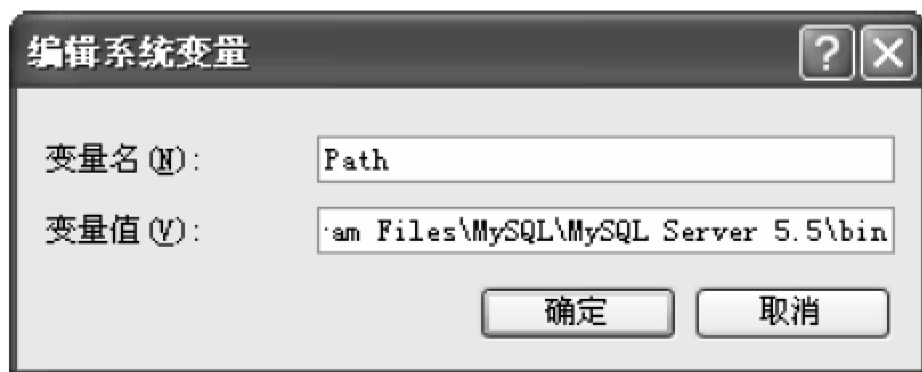


图 15-39　【编辑系统变量】对话框

05 添加完成之后，单击【确定】按钮，这样就完成了配置 PATH 变量的操作，然后就可以直接输入 mysql 命令来登录数据库了。

15.3.2　数据库的创建与删除

MySQL 安装好以后，首先需要创建数据库，这是使用 MySQL 各种功能的前提。本节将详细介绍数据库的基本操作，主要内容包括：创建数据库、删除数据库、不同类型的数据存储引擎和存储引擎的选择。

1. 创建数据库

MySQL 安装完成之后，将会在其 data 目录下自动创建几个必需的数据库，可以使用 SHOW DATABASES;语句来查看当前所有存在的数据库，输入语句如下。

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| test               |
+--------------------+
5 rows in set (0.03 sec)
```

可以看到，数据库列表中包含了 4 个数据库，mysql 是必需的，它描述用户访问权限，test 数

据库经常作为用户试身手的工作，其他数据库这里不作过多介绍。

创建数据库是在系统磁盘上划分一块区域用于数据的存储和管理，如果管理员在设置权限的时候为用户创建了数据库，则可以直接使用，否则需要自己创建数据库。MySQL 中创建数据库的基本 SQL 语法格式为：

```
CREATE DATABASE database_name;
```

“database_name”为要创建的数据库的名称，该名称不能与已经存在的数据库重名。

创建测试数据库 test_db，输入语句如下。

```
CREATE DATABASE test_db;
```

数据库创建好之后，可以使用 SHOW CREATE DATABASE 声明查看数据库的定义。

查看创建好的数据库 test_db 的定义，输入语句如下。

```
mysql> SHOW CREATE DATABASE test_db\G;
*************************** 1. row ***************************
       Database: test_db
Create Database: CREATE DATABASE `test_db` /*!40100 DEFAULT CHARACTER SET utf8 */
1 row in set (0.00 sec)
```

可以看到，如果数据库创建成功，将显示数据库的创建信息。

再次使用 SHOW DATABASES;语句来查看当前所有存在的数据库，输入语句如下。

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| test               |
| test_db            |
+--------------------+
5 rows in set (0.03 sec)
```

可以看到，数据库列表中包含了刚刚创建的数据库 test_db 和其他已经存在的数据库的名称。

2. 删除数据库

删除数据库是将已经存在的数据库从磁盘空间上清除，清除之后，数据库中的所有数据也将一同被删除。删除数据库语句和创建数据库的命令相似，MySQL 中删除数据库的基本语法格式为：

```
DROP DATABASE database_name;
```

“database_name”为要删除的数据库的名称，如果指定的数据库不存在，则删除出错。

删除测试数据库 test_db，输入语句如下。

```
DROP DATABASE test_db;
```

语句执行完毕之后，数据库 test_db 将被删除，再次使用 SHOW CREATE DATABASE 声明查

看数据库的定义，结果如下。

```
mysql> SHOW CREATE DATABASE test  db\G;
ERROR 1049 (42000): Unknown database 'test  db'
ERROR:
No query specified
```

执行结果给出一条错误信息：“ERROR 1049 <42000>：Unknown database 'test_db'”，即数据库 test_db 已不存在，删除成功。



使用 DROP DATABASE 命令时候要非常谨慎，在执行该命令时，MySQL 不会给出任何提醒确认信息，DROP DATABASE 声明删除数据库后，数据库中存储的所有数据表和数据也将一同被删除，而且不能恢复。

下面通过一个案例，让读者全面回顾数据库的基本操作，具体操作介绍如下。

01 登录数据库。

打开 Windows 命令行，输入登录用户名和密码。

```
C:\>mysql –h localhost -u root -p
Enter password: **
```

或者打开 MySQL 5.5 Command Line Client，只输入用户密码也可以登录。登录成功后显示如下信息。

```
Welcome to the MySQL monitor.   Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.5.13 MySQL Community Server (GPL)

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

出现 mysql 命令输入提示符时表示登录成功，可以输入 SQL 语句进行操作。

02 创建数据库 zoo，执行过程如下。

```
mysql> CREATE DATABASE zoo;
Query OK, 1 row affected (0.00 sec)
```

提示信息表明语句成功执行。

查看当前系统中所有的数据库，执行过程如下。

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| test               |
| test_db            |
| zoo                |
+--------------------+
```

可以看到，数据库列表中已经有了名称为 zoo 的数据库，数据库创建成功。

03 选择当前数据库为 zoo，查看数据库 zoo 的信息，执行过程如下。

```
mysql> USE zoo;
Database changed
```

提示信息 Database changed 表明选择成功。

查看数据库信息：

```
mysql> SHOW CREATE DATABASE zoo \G;
*************************** 1. row ***************************
       Database: zoo
Create Database: CREATE DATABASE `zoo` /*!40100 DEFAULT CHARACTER SET utf8 */
```

Database 值表明当前数据库名称，Create Database 值表示创建数据库 zoo 的语句，后面是注释信息。

04 删除数据库 zoo，执行过程如下。

```
mysql> DROP DATABASE zoo;
Query OK, 0 rows affected (0.00 sec)
```

语句执行完毕，将数据库 zoo 从系统中删除。

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| test               |
| test_db            |
+--------------------+
```

可以看到，数据库列表中已经没有名称为 zoo 的数据库。

15.4 项目实战 3：数据库的备份与恢复

尽管采取了一些管理措施来保证数据库的安全，但是不确定的意外情况总是有可能造成数据的损失，例如意外的停电、管理员不小心的操作失误都可能会造成数据的丢失。保证数据安全的最重要的一个措施是确保对数据进行定期备份。如果数据库中的数据丢失或者出现错误，可以使用备份的数据进行还原，这样就尽可能降低了意外原因导致的损失。MySQL 提供了多种方法对数据进行备份和还原。本节将介绍数据备份、数据还原、数据迁移和数据导入导出的相关内容。

15.4.1 数据备份

数据备份是数据库管理员非常重要的工作。系统意外崩溃或者硬件的损坏都可能导致数据库的丢失，因此 MySQL 管理员应该定期地备份数据库，使得在意外情况发生时，尽可能减少损失。下面将介绍数据备份的三种方法。

1. 使用 mysqldump 命令备份

mysqldump 是 MySQL 提供的一个非常有用的数据库备份工具。mysqldump 命令执行时，可以将数据库备份成一个文本文件，该文件中实际上包含了多个 CREATE 和 INSERT 语句，使用这些语句可以重新创建表和插入数据。

mysqldump 备份数据库语句的基本语法格式如下：

```
mysqldump  –u user –h host –ppassword dbname[tbname, [tbname...]]> filename.sql
```

user 表示用户名称；host 表示登录用户的主机名称；password 为登录密码；dbname 为需要备份的数据库名称；tbname 为 dbname 数据库中需要备份的数据表，可以指定多个需要备份的表；右箭头符号“>”告诉 mysqldump 将备份数据表的定义和数据写入到备份文件；filename.sql 为备份文件的名称。

1）使用 mysqldump 备份单个数据库中的所有表

例：在命令行中使用 mysqldump 命令备份数据库中的所有表，将数据备份到 C:\backup 目录下，文件名为“booksdb_20110101.sql”。

```
C:\ >mysqldump -u root -p booksdb > C:\backup\booksdb_20110101.sql
Enter password: **
```

2）使用 mysqldump 备份数据库中的某个表

在前面 mysqldump 语法中介绍，mysqldump 还可以备份数据中的某个表，其语法格式为：

```
mysqldump  –u user –h host –p dbname  [tbname, [tbname...]] > filename.sql
```

tbname 表示数据库中的表名，多个表名之间用空格隔开。

备份表和备份数据库中所有表的语句不同的地方在于，要在数据库名称 dbname 之后指定需要备份的表名称。

例如，备份 booksDB 数据库中的 books 表，输入语句如下。

```
mysqldump -u root -p booksDB books > C:\backup\books_20110101.sql
```

该语句创建名称为 books_20110101.sql 的备份文件，文件中只包含 books 表的 CREATE 和 INSERT 语句。

3）使用 mysqldump 备份多个数据库

如果要使用 mysqldump 备份多个数据库，需要使用--databases 参数，备份多个数据库的语句格式如下。

```
mysqldump  –u user –h host –p --databases  [dbname, [dbname...]] > filename.sql
```

使用--databases 参数之后，必须指定至少一个数据库的名称，多个数据库名称之间用空格隔开。

例如，使用 mysqldump 备份 booksDB 和 test 数据库，输入语句如下。

```
mysqldump -u root -p --databases  booksDB test> C:\backup\books_testDB_20110101.sql
```

该语句创建名称为 books_testDB_20110101.sql 的备份文件，文件中包含了创建两个数据库 boosDB 和 test 所必需的所有语句。

另外，使用--all-databases 参数可以备份系统中所有的数据库，语句如下。

```
mysqldump  –u user –h host –p --all-databases > filename.sql
```

使用参数--all-databases 参数时，不需要指定数据库名称。

例如，使用 mysqldump 备份服务器中的所有数据库，输入语句如下：

```
mysqldump  -u root -p --all-databases > C:\backup\alldbinMySQL.sql
```

该语句创建名称为 alldbinMySQL.sql 的备份文件，文件中包含了对系统中所有数据库的备份信息。


提 示

> 如果在服务器上进行备份，并且表均为 MyISAM 表，应考虑使用 mysqlhotcopy，因为可以更快地进行备份和恢复。

mysqldump 还有一些其他选项可以用来制定备份过程，例如--opt 选项，该选项将打开--quick 、--add-locks、--extended-insert 等多个选项。使用--opt 选项可以提供最快速的数据库转储。

mysqldump 其他常用选项如下：

- --add-drop—database 在每个 CREATE DATABASE 语句前添加 DROP DATABASE 语句。
- --add-drop-tables 在每个 CREATE TABLE 语句前添加 DROP TABLE 语句。
- --add-locking 用 LOCK TABLES 和 UNLOCK TABLES 语句引用每个表转储。重载转储文件时插入得更快。
- --all--database，-A 转储所有数据库中的所有表。与使用---database 选项相同，在命令行中命名所有数据库。
- ---comments[=0|1] 如果设置为 0，禁止转储文件中的其他信息，例如程序版本、服务器版本和主机。--skip—comments 与---comments=0 的结果相同。 默认值为 1，即包括额外信息。
- --compact 产生少量输出。该选项禁用注释并启用--skip-add-drop-tables、--no-set-names、

--skip-disable-keys 和--skip-add-locking 选项。

- --compatible=name 产生与其他数据库系统或旧的 MySQL 服务器更兼容的输出。值可以为 ansi、mysql323、mysql40、postgresql、oracle、mssql、db2、maxdb、no_key_options、no_tables_options 或者 no_field_options。
- --complete-insert，-c 使用包括列名的完整的 INSERT 语句。
- ---debug[=debug_options]，-# [debug_options] 写调试日志。
- --delete，-D 导入文本文件前清空表。
- --default-character-set=charset 使用 charsetas 默认字符集。如果没有指定，mysqldump 使用 utf8。
- --delete-master-logs 在主复制服务器上，完成转储操作后删除二进制日志。该选项自动启用 -master-data。
- --extended-insert，-e 使用包括几个 VALUES 列表的多行 INSERT 语法。这样使转储文件更小，重载文件时可以加速插入。
- --flush-logs，-F 开始转储前刷新 MySQL 服务器日志文件。该选项要求 RELOAD 权限。
- --force，-f 在表转储过程中，即使出现 SQL 错误也继续。
- --lock-all-tables，-x 所有数据库中的所有表加锁。在整体转储过程中通过全局读锁定来实现。该选项自动关闭--single-transaction 和--lock-tables。
- --lock-tables，-l 开始转储前锁定所有表。用 READ LOCAL 锁定表以允许并行插入 MyISAM 表。对于事务表，例如 InnoDB 和 BDB，--single-transaction 是一个更好的选项，因为它根本不需要锁定表。
- --no-create-db，-n 该选项禁用 CREATE DATABASE /*!32312 IF NOT EXISTS*/ db_name 语句，如果给出---database 或--all--database 选项，则包含到输出中。
- --no-create-info，-t 不写重新创建每个转储表的 CREATE TABLE 语句。
- --no-data，-d 不写表的任何行信息，只转储表的结构。
- --opt 该选项是速记。等同于指定--add-drop-tables--add-locking，--create-option，--disable-keys--extended-insert，--lock-tables –quick 和--set-charset。它可以给出很快的转储操作并产生一个可以很快装入 MySQL 服务器的转储文件。该选项默认开启，但可以用--skip-opt 禁用。要想只禁用-opt 启用的选项，使用--skip 形式，例如--skip-add-drop-tables 或--skip-quick。
- --password[=password]，-p[password] 当连接服务器时使用的密码。如果使用短选项形式(-p)，选项和密码之间不能有空格。如果在命令行中--password 或-p 选项后面没有密码值，则提示输入一个密码。
- --port=port_num，-P port_num 用于连接的 TCP/IP 端口号。
- --protocol={TCP | SOCKET | PIPE | MEMORY}使用的连接协议。
- --replace，-r --replace 和--ignore 选项控制复制唯一键值已有记录的输入记录的处理。如果指定--replace，新行替换有相同的唯一键值的已有行。如果指定--ignore，复制已有的唯一键值的输入行被跳过。如果不指定这两个选项，当发现一个复制键值时会出现一个错误，并且忽视文本文件的剩余部分。

- --silent，-s 沉默模式。只有出现错误时才输出。
- --socket=path，-S path 当连接 localhost 时使用的套接字文件为默认主机。
- --user=user_name，-u user_name 当连接服务器时 MySQL 使用的用户名。
- --verbose，-v 冗长模式。打印出程序操作的详细信息。
- --version，-V 显示版本信息并退出。
- --xml，-X 产生 XML 输出。

mysqldump 提供许多选项，包括用于调试和压缩的。在这里只是列举最有用的。运行帮助命令 mysqldump --help，可以获得特定版本的完整选项列表。



提　示

如果运行 mysqldump 没有--quick 或--opt 选项，mysqldump 在转储结果前将整个结果集装入内存。如果转储大数据库可能会出现问题。该选项默认启用，但可以用--skip-opt 禁用。如果使用最新版本的 mysqldump 程序备份数据，并用于还原到比较旧版本的 MySQL 服务器中，则不要使用--opt 或-e 选项。

2. 直接复制整个数据库目录

因为 MySQL 表保存为文件方式，所以可以直接复制 MySQL 数据库的存储目录及文件进行备份。MySQL 的数据库目录位置不一定相同，在 Windows 平台下 MySQL 5.5 存放数据库的目录通常默认为“C:\Documents and Settings\All Users\Application Data\MySQL\MySQL Server 5.5\data”或者其他用户自定义目录；在 Linux 平台下，数据库目录位置通常为/var/lib/mysql/，不同 Linux 版本下目录会有不同，读者应在自己使用的平台下查找该目录。

这是一种简单、快速、有效的备份方式。要想保持备份的一致性，备份前需要对相关表执行 LOCK TABLES 操作，然后对表执行 FLUSH TABLES。这样当复制数据库目录中的文件时，允许其他客户继续查询表。需要 FLUSH TABLES 语句来确保开始备份前将所有激活的索引页写入硬盘。当然，也可以停止 MySQL 服务再进行备份操作。

这种方法虽然简单，但并不是最好的方法，因为这种方法对 InnoDB 存储引擎的表不适用。使用这种方法备份的数据最好还原到相同版本的服务器中，不同的版本可能不兼容。



提　示

在 MySQL 版本号中，第一个数字表示主版本号，主版本号相同的 MySQL 数据库文件格式相同。

3. 使用 mysqlhotcopy 工具快速备份

mysqlhotcopy 是一个 Perl 脚本，最初由 Tim Bunce 编写并提供。它使用 LOCK TABLES、FLUSH TABLES 和 cp 或 scp 来快速备份数据库。它是备份数据库或单个表的最快的途径，但它只能运行在数据库目录所在的机器上，并且只可以备份 MyISAM 类型的表。mysqlhotcopy 在 UNIX 系统中运行。

mysqlhotcopy 命令语法格式如下。

```
mysqlhotcopy db_name_1, ..., db_name_n   /path/to/new_directory
```

da_name1, …, da_name_n 分别为需要备份的数据库的名称；/path/to/new_directory 指定备份文件目录。

例：使用 mysqlhotcopy 备份 test 数据库到/usr/backup 目录下，输入语句如下。

```
mysqlhotcopy   -u root –p test /usr/backup
```

要想执行 mysqlhotcopy，必须可以访问备份的表文件，具有那些表的 SELECT 权限、RELOAD 权限（以便能够执行 FLUSH TABLES）和 LOCK TABLES 权限。



提 示

mysqlhotcopy 只是将表所在的目录复制到另一个位置，只能用于备份 MyISAM 和 ARCHIVE 表。备份 InnoDB 类型的数据表时会出现错误信息。由于其复制本地格式的文件，故也不能移植到其他硬件或操作系统下。

15.4.2　数据还原

管理人员操作的失误、计算机故障以及其他意外情况，都会导致数据的丢失和破坏。当数据丢失或意外破坏时，可以通过还原已经备份的数据尽量减少数据丢失和破坏造成的损失。下面将介绍三种数据还原的方法。

1. 使用 mysql 命令还原

对于已经备份的包含 CREATE、INSERT 语句的文本文件，可以使用 mysql 命令导入到数据库中。本小节将介绍 mysql 命令导入 sql 文件的方法。

备份的 sql 文件中包含 CREATE、INSERT 语句（有时也会有 DROP 语句）。mysql 命令可以直接执行文件中这些语句，语法如下。

```
mysql –u user –p [dbname] < filename.sql
```

user 是执行 backup.sql 中语句的用户名；-p 表示输入用户密码；dbname 是数据库名。如果 filename.sql 文件为 mysqldump 工具创建的包含创建数据库语句的文件，执行的时候不需要指定数据库名。

例：使用 mysql 命令将 C:\backup\booksdb_20110101.sql 文件中的备份导入到数据库中，输入语句如下。

```
mysql –u root –p booksDB < C:\backup\booksdb_20110101.sql
```

执行该语句前，必须先在 MySQL 服务器中创建 booksDB 数据库，如果不存在恢复过程将会出错。命令执行成功之后 booksdb_20110101.sql 文件中的语句就会在指定的数据库中恢复以前的表。

如果已经登录 MySQL 服务器，还可以使用 source 命令导入 sql 文件。source 语句语法如下。

```
source filename
```

例如使用 root 用户登录到服务器，然后使用 source 导入本地的备份文件 booksdb_20110101.sql，输入语句如下：

```
mysql> use booksdb;                        //选择要恢复到的数据库
Database changed                           //使用 source 命令导入备份文件
```

```
mysql> source C:/backup/booksdb_20110101.sql
```

命令执行后，会列出备份文件 booksdb_20110101.sql 中每一条语句的执行结果。source 命令执行成功后，booksdb_20110101.sql 中的语句会全部导入到现有数据库中。



执行 source 命令前，必须使用 use 语句选择数据库。不然，恢复过程中会出现“ERROR 1046 (3D000): No database selected” 的错误。

2. 直接复制到数据库目录

如果数据库通过复制数据库文件备份，可以直接复制备份的文件到 MySQL 数据目录下实现还原。通过这种方式还原时，必须保存备份数据的数据库和待还原的数据库服务器的主版本号相同。而且这种方式只对 MyISAM 引擎的表有效，对于 InnoDB 引擎的表不可用。

执行还原之前关闭 mysql 服务，将备份的文件或目录覆盖 MySQL 的 data 目录，启动 mysql 服务。对于 Linux/UNIX 操作系统来说，复制完文件需要将文件的用户和组更改为 mysql 运行的用户和组，通常用户是 mysql，组也是 mysql。

3. mysqlhotcopy 快速恢复

mysqlhotcopy 备份后的文件也可以用来恢复数据库，在 MySQL 服务器停止运行时，将备份的数据库文件拷贝到 MySQL 存放数据的位置（MySQL 的 Data 文件夹），重新启动 MySQL 服务即可。如果以根用户执行该操作，必须指定数据库文件的所有者，输入语句如下。

```
chown -R mysql.mysql /var/lib/mysql/dbname
```

例：从 mysqlhotcopy 拷贝的备份恢复数据库，输入语句如下。

```
cp –R   /usr/backup/test usr/local/mysql/data
```

执行完该语句，重启服务器，MySQL 将恢复到备份状态。



如果需要恢复的数据库已经存在，则需要使用 DROP 语句删除已经存在的数据库，恢复才能成功。另外 MySQL 不同版本之间必须兼容，恢复之后的数据才可以使用。

15.4.3 数据库迁移

数据库迁移就是把数据从一个系统移动到另一个系统上。数据迁移有以下原因。

（1）需要安装新的数据库服务器。

（2）MySQL 版本更新。

（3）数据库管理系统的变更（如从 Microsoft SQL Server 迁移到 MySQL）。

下面来介绍三类数据库迁移的方法。

1. 相同版本的 MySQL 数据库之间的迁移

相同版本的 MySQL 数据库之间的迁移就是在主版本号相同的 MySQL 数据库之间进行数据库移动。迁移过程其实就是源数据库备份和目标数据库还原过程的组合。

在讲解数据库备份和还原时，已经知道最简单的方式是通过复制数据库文件目录，但是此种方法只适用于 MyISAM 引擎的表。而对于 InnoDB 表，不能用直接复制文件的方式备份数据库，因此最常用和最安全的方式是使用 mysqldump 命令导出数据，然后在目录数据库服务器使用 mysql 命令导入。

例：将 www.abc.com 主机上的 MySQL 数据库全部迁移到 www.bcd.com 主机上。在 www.abc.com 主机上执行的命令如下。

```
mysqldump –h www.bac.com –uroot –ppassword    dbname |
mysql –hwww.bcd.com –uroot –ppassword
```

mysqldump 导入的数据直接通过管道符“｜”传给 mysql 命令导入到主机 www.bcd.com 数据库中，dbname 为需要迁移的数据库名称，如果要迁移全部的数据库，可使用参数--all-databases。

2. 不同版本的 MySQL 数据库之间的迁移

由于数据库升级等原因，需要将较旧版本 MySQL 数据库中的数据迁移到的较新版本的数据库中。MySQL 服务器升级时，需要先停止服务，然后卸载旧版本，并安装新版的 MySQL，这种更新方法很简单，如果想保留旧版本中用户访问控制信息，则需要备份 MySQL 中的 mysql 数据库，在新版本 MySQL 安装完成之后，重新读入 mysql 备份文件中的信息。

旧版本与新版本的 MySQL 可能使用不同的默认字符集，例如 MySQL 4.x 中大多使用 latin1 作为默认字符集，而 MySQL 5.x 的默认字符集为 utf8。如果数据库中有中文数据的，迁移过程中需要对默认字符集进行修改，不然可能会无法正常显示的结果。

新的版本会对旧版本有一定兼容性。从旧版本的 MySQL 向新版本的 MySQL 迁移时，对于 MyISAM 引擎的表，可以直接复制数据库文件，也可以使用 mysqlhotcopy 工具、mysqldump 工具。对于 InnoDB 引擎的表，一般只能使用 mysqldump 将数据导出。然后使用 mysql 命令导入到目标服务器上。从新版本向旧版本 MySQL 迁移数据时要特别小心，最好使用 mysqldump 命令导出，然后导入后目标数据库中。

3. 不同数据库之间迁移

不同类型的数据库之间的迁移，是指从把 MySQL 的数据库转移到其他类型的数据库，例如从 MySQL 迁移到 Oracle，从 Oracle 迁移到 MySQL，从 MySQL 迁移到 sqlserver 等。

迁移之前，需要了解不同数据库的架构，比较它们之间的差异。不同数据库中表示定义相同类型的数据的关键字可能会不同。例如，MySQL 中日期字段分为 DATE 和 TIME 两种，而 Oracle 日期字段只有 DATE。另外数据库厂商并没有完全按照 SQL 标准来设计数据库系统，导致不同的数据库系统的 SQL 语句有差别。例如，MySQL 几乎完全支持标准 SQL 语言，而 Microsoft SQL Server 使用的是 T-SQL 语言，T-SQL 中有些非标准的 SQL 语句，因此在迁移时必须对这些语句进行语句映射处理。

数据库迁移可以使用一些工具，例如 Windows 系统下可以使用 MyODBC 实现 MySQL 和 SQL Server 之间的迁移。MySQL 官方提供的工具 MySQL Migration Toolkit 也可以在不同数据库间进行数据迁移。

15.4.4 综合案例

备份有助于保护数据库，通过备份可以完整保存 MySQL 中各个数据库的特定状态。通过还原恢复数据库中的数据，防止在系统出现故障、数据丢失或者不合理操作对数据库造成的灾难。作为 MySQL 的管理人员，应该定期备份所有活动的数据库，以免发生数据丢失。因此无论怎样强调数据库的备份工作都不过分。下面介绍一个综合案例，使读者进一步了解数据库备份与还原的方法与过程。

01 使用 mysqldump 命令将 suppliers 表备份到文件 C:\bktestdir\suppliers_bk.sql。

首先创建系统目录，在系统 C 盘下面新建文件夹 bktestdir，然后打开命令行窗口，输入语句如下：

```
C:\ >mysqldump -u root -p test suppliers > C:\bktestdir\suppliers  bk.sql
Enter password: **
```

语句执行完毕，打开目录 C:\bktestdir，可以看到已经创建好的备份文件 suppliers_bk.sql，内容如下：

```
-- MySQL dump 10.13    Distrib 5.5.13, for Win32 (x86)
--
-- Host: localhost        Database: test
-- ------------------------------------------------------
-- Server version   5.5.13

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD  COLLATION  CONNECTION=@@COLLATION  CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD  TIME  ZONE=@@TIME  ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD  FOREIGN  KEY  CHECKS=@@FOREIGN  KEY  CHECKS, FOREIGN  KEY
CHECKS=0 */;
/*!40101 SET @OLD  SQL  MODE=@@SQL  MODE, SQL  MODE='NO  AUTO  VALUE  ON  ZERO'*/;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;


--
-- Table structure for table `suppliers`
--

DROP TABLE IF EXISTS `suppliers`;
/*!40101 SET @saved  cs  client        = @@character  set  client */;
/*!40101 SET character  set  client = utf8 */;
CREATE TABLE `suppliers` (
  `s_id` int(11) NOT NULL AUTO_INCREMENT,
```

```
  `s_name` char(50) NOT NULL,
  `s_city` char(50) DEFAULT NULL,
  `s_zip` char(10) DEFAULT NULL,
  `s_call` char(50) NOT NULL,
  PRIMARY KEY (`s_id`)
) ENGINE=InnoDB AUTO_INCREMENT=108 DEFAULT CHARSET=utf8;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `suppliers`
--

LOCK TABLES `suppliers` WRITE;
/*!40000 ALTER TABLE `suppliers` DISABLE KEYS */;
INSERT INTO `suppliers` VALUES (101,'FastFruit Inc.','Tianjin','463400','48075'),(102,'LT Supplies','Chongqin
g','100023','44333'),(103,'ACME','Shanghai','100024','90046'),(104,'FNK Inc.','Zhongshan','212021','11111'),(105,
'Good Set','Taiyuang','230009','22222'),(106,'Just Eat Ours','Beijing','010','45678'),(107,'DK Inc.','Qingdao','23000
9','33332');
/*!40000 ALTER TABLE `suppliers` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2011-08-20 15:07:44
```

02 使用 mysql 命令将备份文件 suppliers_bk.sql 中的数据还原 suppliers 表。

为了验证还原之后数据的正确性，删除 suppliers 表中的所有记录，登录 MySQL，输入语句：

```
mysql> USE test;
Database changed
mysql> DELETE FROM suppliers;
Query OK, 7 rows affected (0.00 sec)
```

此时，suppliers 表中不再有任何数据记录，在 MySQL 命令行输入还原语句如下：

```
mysql> source C:/bktestdir/suppliers_bk.sql;
```

语句执行过程中会出现多行提示信息，执行成功之后使用 SELECT 语句查询 suppliers 表内容如下：

```
mysql> SELECT * FROM suppliers;
+------+----------------+-------------+---------+--------+
| s_id | s_name         | s_city      | s_zip   | s_call |
+------+----------------+-------------+---------+--------+
```

```
|   101 | FastFruit Inc. | Tianjin     | 463400 | 48075|
|   102 | LT Supplies    | Chongqing | 100023 | 44333|
|   103 | ACME           | Shanghai   | 100024 | 90046|
|   104 | FNK Inc.       | Zhongshan | 212021 | 11111|
|   105 | Good Set       | Taiyuang   | 230009 | 22222|
|   106 | Just Eat Ours | Beijing     | 010     | 45678 |
|   107 | DK Inc.        | Qingdao     | 230009 | 33332 |
+------+----------------+-------------+---------+--------+
7 rows in set (0.00 sec)
```

由查询结果可以看到，还原操作成功。

03 使用 SELECT… INTO OUTFILE 语句导出 suppliers 表中的记录，导出文件位于目录 C:\bktestdir 下，名称为 suppliers_out.txt。

执行过程如下：

```
mysql> SELECT * FROM test.suppliers INTO OUTFILE "C:/bktestdir/suppliers_out.txt"
    -> FIELDS
    -> TERMINATED BY ','
    -> ENCLOSED BY '\"'
    -> LINES
    -> STARTING BY '<'
    -> TERMINATED BY '>\r\n';
Query OK, 7 rows affected (0.00 sec)
```

TERMINATED BY ','指定不同字段之间使用逗号分隔开；ENCLOSED BY '\"'指定字段值使用双引号括起来；STARTING BY '< '指定每行记录以左箭头符号开始；TERMINATED BY ' >\r\n';指定每行记录以右箭头符号和回车换行符介绍。语句执行完毕，打开目录 C:\bktestdir，可以看到已经创建好的导出文件 suppliers_out.txt，内容如下：

```
<"101","FastFruit Inc.","Tianjin","463400","48075">
<"102","LT Supplies","Chongqing","100023","44333">
<"103","ACME","Shanghai","100024","90046">
<"104","FNK Inc.","Zhongshan","212021","11111">
<"105","Good Set","Taiyuang","230009","22222">
<"106","Just Eat Ours","Beijing","010","45678">
<"107","DK Inc.","Qingdao","230009","33332">
```

04 使用 LOAD DATA INFILE 语句导入 suppliers_out.txt 数据到 suppliers 表。

首先使用 DELETE 语句删除 suppliers 表中的所有记录，然后输入导入语句：

```
mysql> LOAD DATA INFILE 'C:/bktestdir/suppliers_out.txt' INTO TABLE test.suppliers
    -> FIELDS
    -> TERMINATED BY ','
    -> ENCLOSED BY '\"'
    -> LINES
    -> STARTING BY '<'
    -> TERMINATED BY '>\r\n';
Query OK, 7 rows affected (0.00 sec)
```

```
Records: 7    Deleted: 0    Skipped: 0    Warnings: 0
```

语句执行之后，suppliers_out.txt 文件中的数据将导入 suppliers 表中，由于导出 txt 文件时指定了一些特殊字符，因此还原语句中也要指定这些字符，已确保还原后数据的完整性和正确性。

05 使用 mysqldump 命令将 suppliers 表中的记录导出到文件 C:\bktestdir\suppliers_html.html。

导出表数据到 html 文件，使用 mysql 命令时需要指定--html 选项，在 Windows 命令行窗口输入导出语句如下：

```
mysqldump -u root -p --html --execute="SELECT * FROM suppliers;" test > C:/bktestdir/suppliers_html.html
```

语句执行完毕，打开目录 C:\bktestdir，可以看到已经创建好的导出文件 suppliers_html.html，读者可以使用浏览器打开该文件，在浏览器中显示格式和内容如表 15-1 所示。

表 15-1　浏览器中显示导出文件的内容

s_id	s_name	s_city	s_zip	s_call
101	FastFruit Inc.	Tianjin	463400	48075
102	LT Supplies	Chongqing	100023	44333
103	ACME	Shanghai	100024	90046
104	FNK Inc.	Zhongshan	212021	11111
105	Good Set	Taiyuang	230009	22222
106	Just Eat Ours	Beijing	010	45678
107	DK Inc.	Qingdao	230009	33332

15.5　专家答疑

计算机技术具有很强的操作性，MySQL 的安装和配置是一件非常简单的事，但是操作过程也有可能出现问题，读者需要多实践、多总结。

（1）MySQL 必须注册为系统服务吗？

答：使用配置向导时，可以将 MySQL 注册为系统服务，MySQL 会随 Windows 的启动而自动启动。这样就免除了每次手动输入启动命令的麻烦，如果不想安装服务，取消选中 Install As Windows Service 复选框。如果读者不需要经常使用 MySQL，可以在配置向导中不选中 Launch the MySQL Server automatically 复选框，根据需要使用 net 命令启动或者关闭 MySQL 服务，这样也减少了系统资源的浪费。

（2）MySQL 安装失败怎么办？

答：安装过程失败，多是由于重新安装 MySQL 的缘故，MySQL 在删除的时候，不能自动删除相关的信息。解决方法是，把以前安装目录删除掉。删除在 C 盘的 program file 文件夹里面 mysql 的安装目录文件夹；同时删除 MySQL 的 DATA 目录，该目录一般为隐藏文件，其位置一般在“C:\Documents and Settings\All Users\Application Data\ MySQL”目录下，删除掉后重新安装即可。

（3）mysqldump 备份的文件只能在 MySQL 中使用吗？

答：mysqldump 备份的文本文件实际是数据库的一个副本，使用该文件不仅可以在 MySQL 中恢复数据库，而且通过对该文件的简单修改，可以使用该文件在 SQL Server 或者 Sybase 等其他数据库中恢复数据库。这在某种程度上实现了数据库之间的迁移。

（4）如何选择备份工具？

答：直接拷贝数据文件是最为直接、快速的备份方法，但缺点是基本上不能实现增量备份。备份时必须确保没有使用这些表。如果在拷贝一个表的同时服务器正在修改它，则拷贝无效。备份文件时，最好关闭服务器，然后重新启动服务器。为了保证数据的一致性，需要在备份文件前，执行以下 SQL 语句：

```
FLUSH TABLES WITH READ LOCK;
```

也就是把内存中的数据都刷新到磁盘中，同时锁定数据表，以保证拷贝过程中不会有新的数据写入。这种方法备份出来的数据恢复也很简单，直接拷贝回原来的数据库目录下即可。

mysqlhotcopy 是一个 PERL 程序，它使用 LOCK TABLES、FLUSH TABLES 和 cp 或 scp 来快速备份数据库。它是备份数据库或单个表的最快的途径，但它只能运行在数据库文件所在的机器上，并且 mysqlhotcopy 只能用于备份 MyISAM 表。mysqlhotcopy 适合于小型数据库的备份，数据量不大，可以使用 mysqlhotcopy 程序每天进行一次完全备份。

mysqldump 将数据表导成 SQL 脚本文件，在不同的 MySQL 版本之间升级时相对比较合适，这也是最常用的备份方法。mysqldump 比直接拷贝要慢些。

（5）使用 mysqldump 备份整个数据库成功，把表和数据库都删除了，但使用备份文件却不能恢复数据库？

答：出现这种情况，是因为备份的时候没有指定--databases 参数，默认情况下，如果只指定数据库名称，mysqldump 备份的是数据库中所有的表，而不包括数据库创建语句，例如：

```
mysqldump -u root -p booksdb > c:/backup/booksdb_20110101.sql
```

该语句只备份了 booksdb 数据库下所有的表，读者打开该文件可以看到，文件中不包含创建 booksdb 数据库的 CREATE DATABASE 语句，因此如果把 booksdb 也删除了，使用该 sql 文件不能还原以前的表，还原时会出现 ERROR 1046 (3D000): No database selected 的错误信息。必须在 MySQL 命令行下创建 booksdb 数据库，并使用 use 语句选择 booksdb 之后才可以还原。而下面的语句，数据库删除之后，可以正常还原备份时的状态。

```
mysqldump -u root -p --databases    booksDB > C:\backup\books_DB_20110101.sql
```

该语句不仅备份了所有数据库下的表结构，而且包括了创建数据库的语句。

第 16 章　SolarWinds 网管工具的使用

在进行网络管理时，为了提高管理效率网络管理员往往会使用一些管理工具。为了实现各种管理功能，管理工具的种类也多种多样。本章将介绍一个网络管理工具集——SolarWinds，该程序由许多小的网络管理工具组成。

16.1　SolarWinds 工具介绍

在使用 SolarWinds 之前，首先来简单了解一下 SolarWinds 工具及其使用环境。

16.1.1　SolarWinds 网管工具概述

SolarWinds 是一款非常出色的网络工具箱，该工具箱中包含了非常全面的网络管理工具，能协助网络管理员完成大部分的网络管理工作，并且可以大幅简化网络管理员对于网络的管理工作负担，提升网管效率。

SolarWinds 所能够使用的工具可以分为以下几类。

1. 网络发现类

IP 网络浏览器（IP Network Browser）工具、Ping Sweep 工具、子网列表（Subnet List）工具、DNS 核查（DNS Audit）工具、IP 地址管理（IP Address Management）工具和 MAC 地址发现（MAC Address Discovery）工具等。

2. 网络性能监控类

网络性能监控器（Network Performance Monitor）工具、CPU 测量（CPU Gauge）工具、带宽监控（Bandwidth Monitor）工具、路由 CPU 负荷（Router CPU Load）工具和带宽测量（Bandwidth Gauges ）工具等。

3. 网络监控类

Watch It!工具、网络监控器（Network Monitor）工具、Syslog 服务器工具、路由 CPU 负荷（Router CPU Load）工具、高级 ping 工具和网络性能监控器（Network Performance Monitor）工具等。

4. 用于 Cisco 网络的工具

路由 CPU 负荷（Router CPU Load）工具、IP 网络浏览器（IP Network Browser）工具、配置下载（Config Downloader）工具、配置上传（Config Uploader）工具、配置编辑器/浏览器（Config Editor/Viewer）工具、Proxy Ping（代理 Ping）工具、路由器密码加密术（Router Password Decryption）工具、CPU 测量（CPU Gauge）工具和路由器安全检查（Router Security Check）工具等。

5. IP 地址管理类

子网计算器（Advanced Subnet Calculator）工具、DNS 解析（DNS / Who Is Resolver）工具、DNS 核查（DNS Audit）工具、IP 地址管理（IP Address Management）工具等。

6. 安全类

路由安全性检查（Router Security Check）工具、TCP Reset 工具、SNMP Brute Force 攻击工具、SNMP 词典攻击（Dictionary Attack）工具和路由器密码加密术（Router Password Decryption）工具。

7. Ping 类

Ping 工具、高级 ping 工具、Trace Route 工具、Proxy Ping 工具、Ping Sweep 工具。

8. MIB 浏览器类

MIB Walk 工具、更新系统 MIBs（Update System MIBs）工具、MIB 浏览器（MIB Viewer ）工具和 SNMP 图像工具。

16.1.2 项目实战 1：配置 SNMP 网络管理协议

网络环境中的设备种类比较多，想要对所有设备进行管理，必须要先开启这些设备的网络管理协议（SNMP）。下面主要对 Windows 、Linux 、Cisco 路由器三种常见设备的 SNMP 协议开启、配置方法进行介绍。

1. 开启 Windows 的 SNMP 协议

安装 Windows 操作系统的主机在网络中使用的比例比较大，常见的有 Windows XP、Windows Server 2003、Windows Server 2008、Windows 7 等，但是无论哪一个版本的 Windows 系统，其安装、配置 SNMP 的方法都是相似的。下面以 Windows Server 2003 为例进行介绍。

1）安装 SNMP 组件

大部分的 Windows 操作系统是没有安装 SNMP 组件的，所以首先要进行 SNMP 的组件安装，具体操作步骤如下。

01 选择【开始】➢【设置】➢【控制面板】命令。

02 弹出【控制面板】窗口，选择【添加或删除程序】选项。

03 弹出【添加或删除程序】窗口，如图 16-1 所示，在左侧的列表中选择【添加/删除 Windows 组件】选项。

04 弹出【Windows 组件向导】对话框，如图 16-2 所示，在【组件】列表框中双击【管理和监视工具】选项。



图 16-1　【添加或删除程序】窗口



图 16-2　【Windows 组件向导】对话框

05 弹出【管理和监视工具】对话框，如图 16-3 所示，选中【简单网络管理协议（SNMP）】复选框，单击【确定】按钮。

06 返回【Windows 组件向导】对话框，如图 16-4 所示，选中【管理和监视工具】复选框，单击【下一步】按钮。

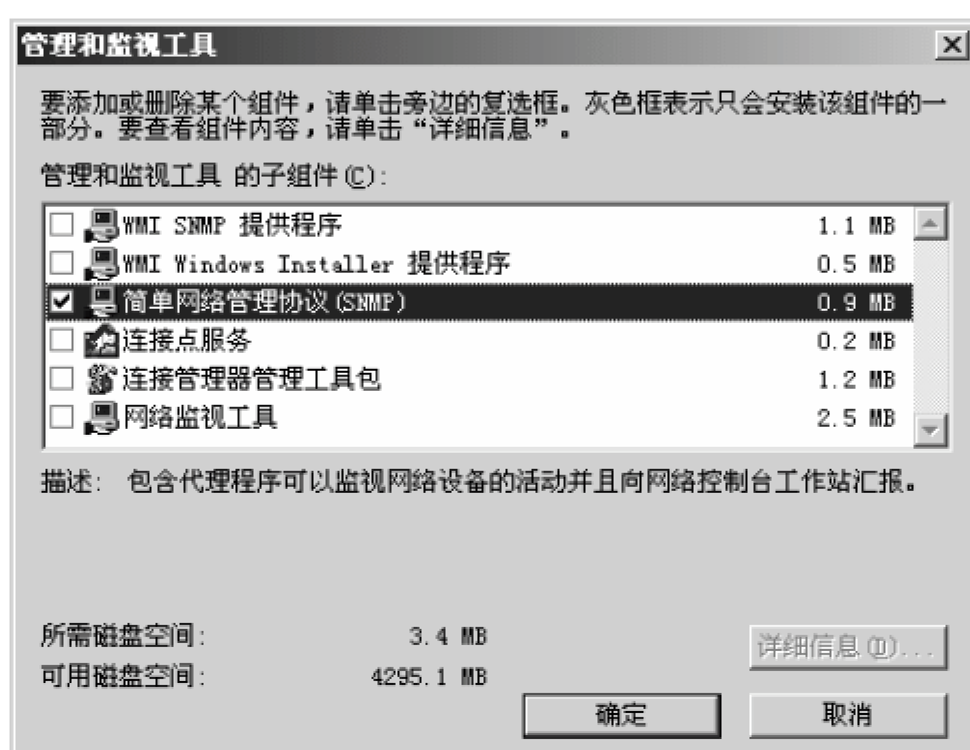




图 16-3　【管理和监视工具】对话框　　图 16-4　【Windows 组件向导】对话框

07 系统自动安装已选组件，并显示安装进度，如图 16-5 所示。

08 组件安装完成后，如图 16-6 所示，单击【完成】按钮。



图 16-5 【正在配置组件】对话框



图 16-6 安装完成窗口

2）配置 SNMP 服务项

安装 SNMP 组件后，默认可以直接使用，但是不同的网络管理环境要求或管理参数配置不尽相同，所以在使用之前，首先要保证 SNMP 服务的正确可用。

配置 SNMP 服务的具体操作步骤如下。

01 选择【开始】➢【运行】命令。弹出【运行】对话框，在【打开】文本框中输入“services.msc”命令，单击【确定】按钮。

02 弹出【服务】窗口，在右侧系统服务列表中可以找到 SNMP Service（SNMP 服务）和 SNMP Trap Service（SNMP 陷阱）服务项，两个服务均处于【已启动】状态，说明当前主机的 SNMP 服务可用，双击 SNMP Service（SNMP 服务）服务项，如图 16-7 所示。



图 16-7 【服务】窗口

03 弹出【SNMP Service 的属性（本地计算机）】对话框，打开【陷阱】选项卡，如图 16-8 所示。

04 当主机出现异常时，可以通过陷阱服务将异常现象主动反馈给 SNMP 管理服务器，在【团体名称】文本框中输入有效团体名，本实例采用默认值“public”，单击【添加】按钮，如图 16-8 所示。

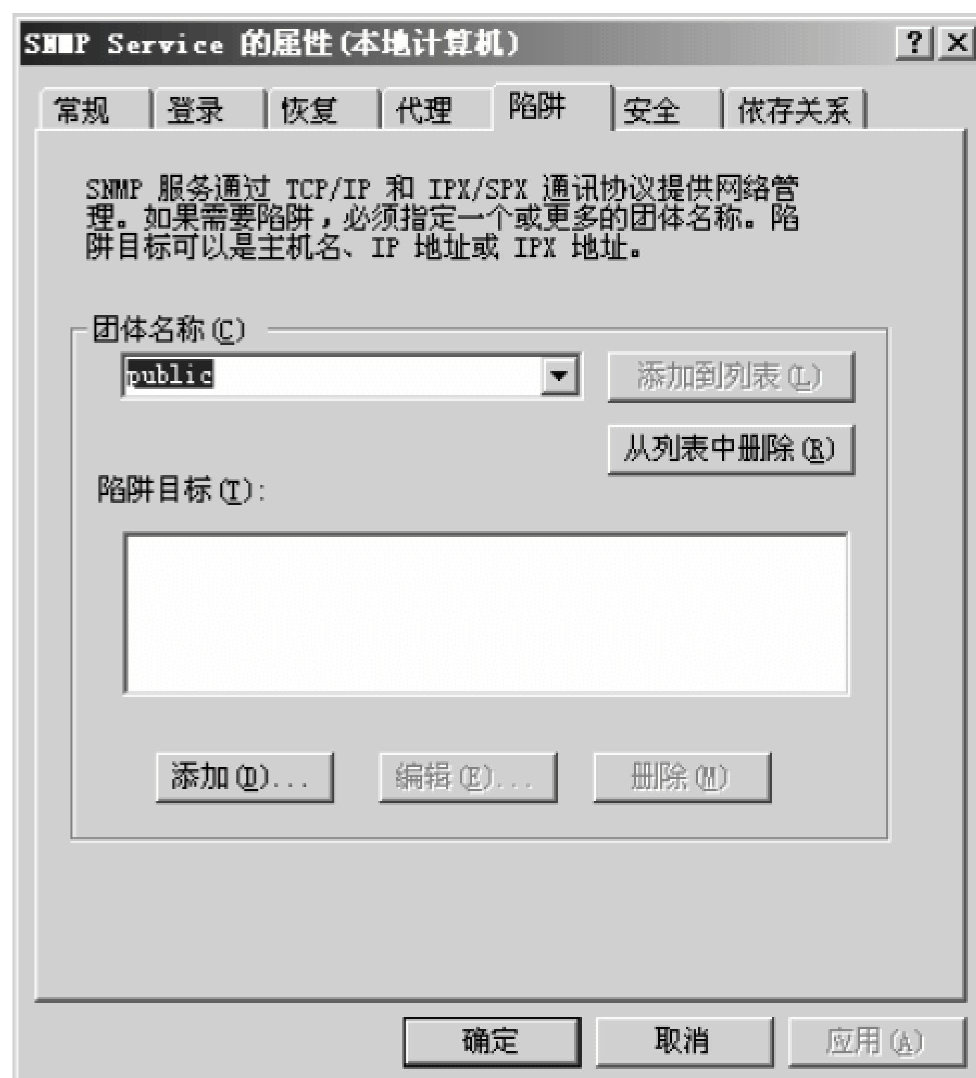


图 16-8 【陷阱】选项卡

05 弹出【SNMP 服务配置】对话框，在【主机名，IP 或 IPX 地址】文本框中输入陷阱目标主机地址，一般为网络管理服务器的主机地址，单击【添加】按钮，如图 16-9 所示。

06 返回【陷阱】选项卡，在【陷阱目标】列表中显示新添加的陷阱目标主机地址，如图 16-10 所示。



图 16-9 【SNMP 服务配置】对话框

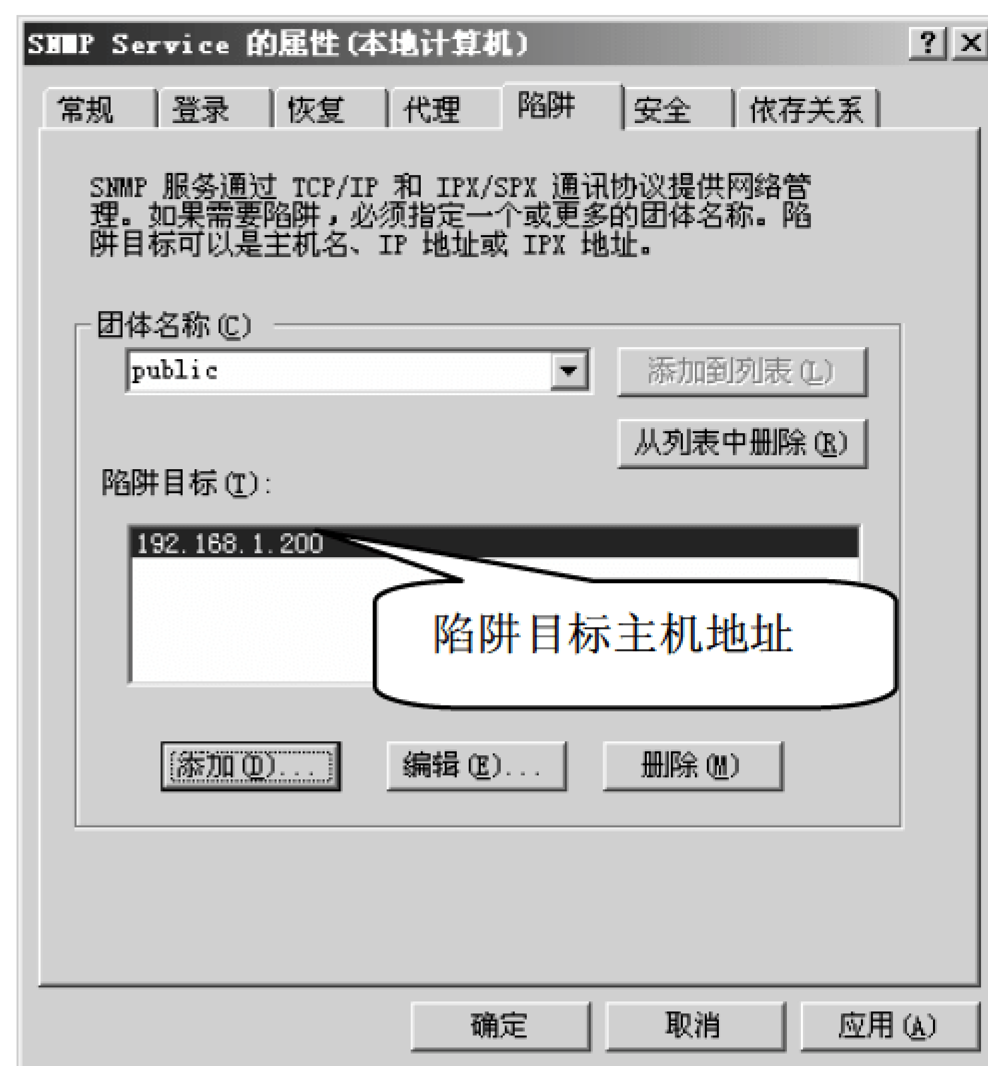


图 16-10 【SNMP Service 的属性】对话框

07 选择【安全】选项卡，在【接受团体名称】列表中显示了可用团体名，默认团体名为“pubic”，权限为“读写”，单击【添加】按钮，如图 16-11 所示。

08 弹出【SNMP 服务配置】对话框，在【团体名称】文本框中可以输入新的可用团体名，如图 16-12 所示。

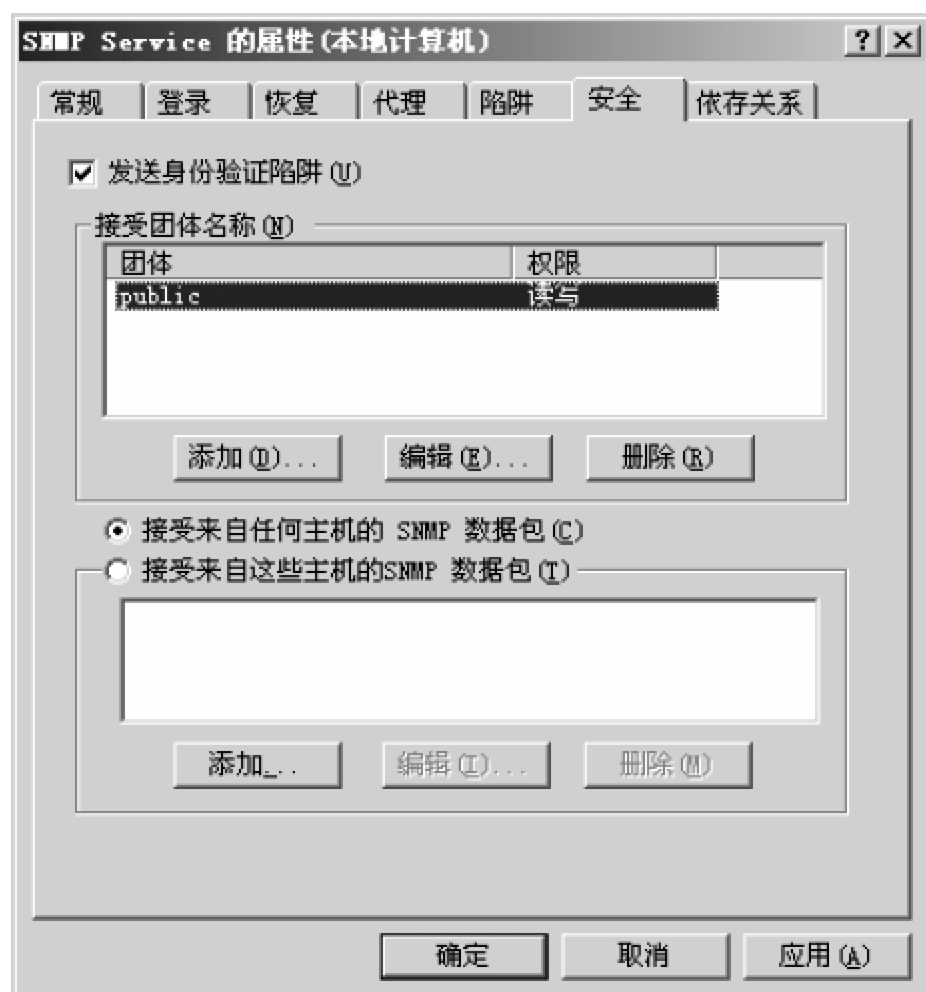


图 16-11 【安全】选项卡

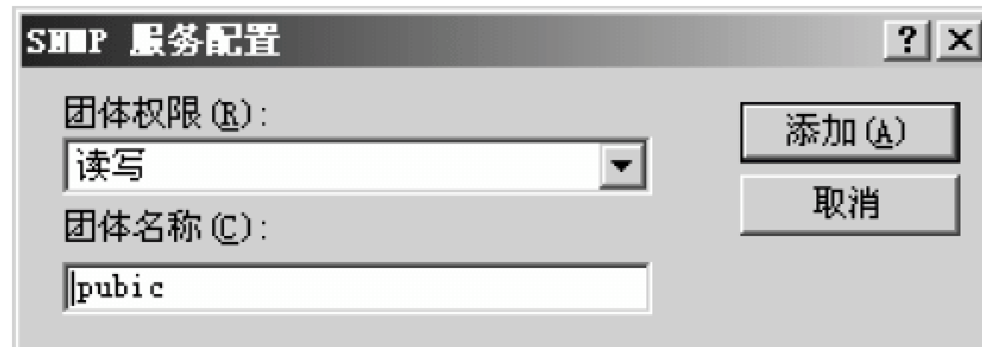


图 16-12 【SNMP 服务配置】对话框

09 在【团体权限】下拉列表框中，可以根据实际需求设定对应团体名的权限，单击【确定】按钮，如图 16-13 所示。

10 返回【安全】选项卡，本实例添加了一个团体名为 SNMP，权限为“只读”的接受团体名称，单击【确定】按钮，完成 SNMP 服务的设置，如图 16-14 所示。

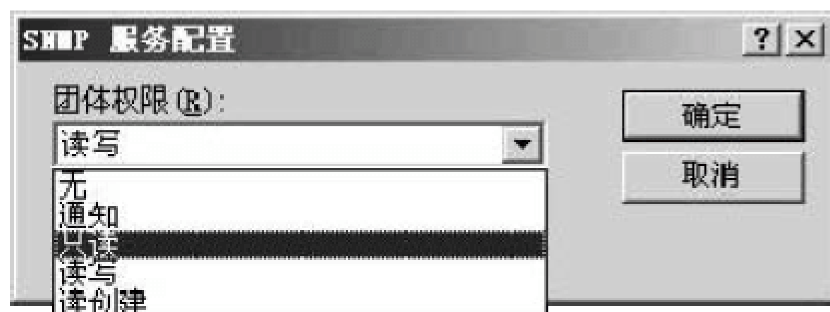


图 16-13 设定团体权限

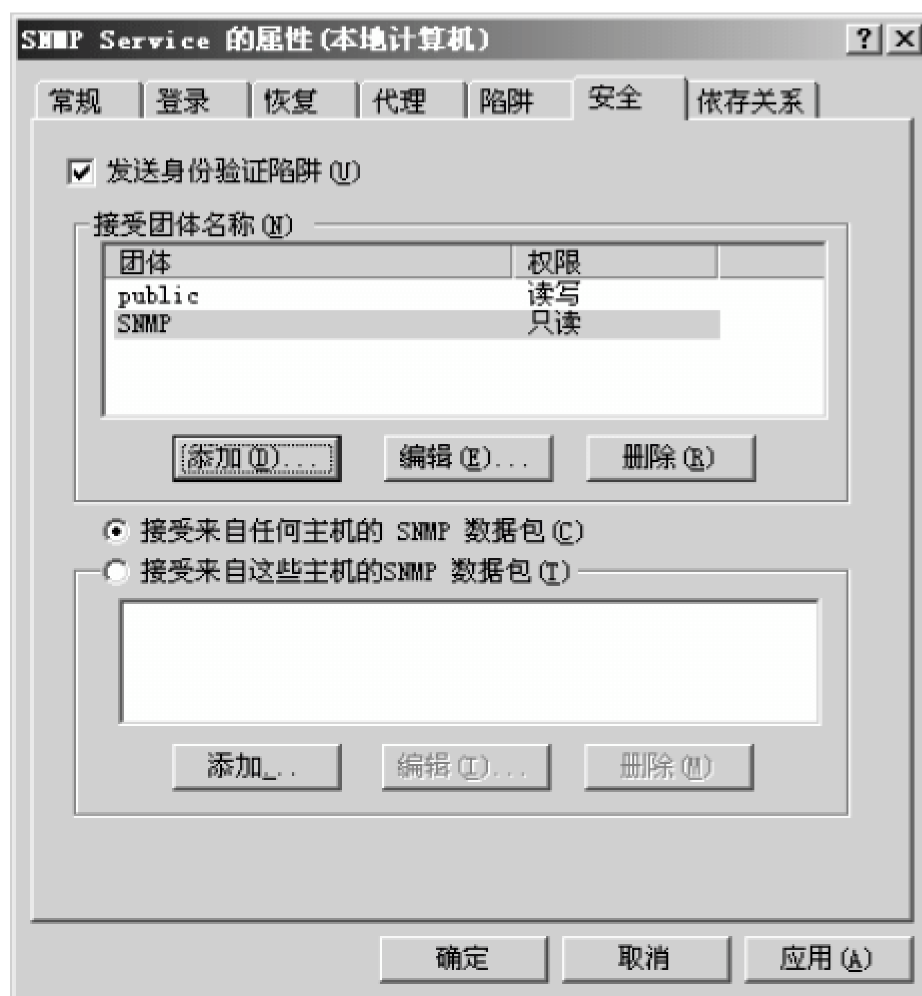


图 16-14 完成 SNMP 服务的设置

2. 开启 Linux 的 SNMP 协议

Linux 系统的版本比较多，很多系统默认没有安装 SNMP 软件包，需要进行手动安装。SNMP 软件包比较小，本实例采用 RPM 包安装方法，下面介绍其具体的安装与配置方法。

1）安装 SNMP 软件包

SNMP 主要安装两个包，分别是 net-snmp-libs 和 net-snmp，将软件包下载到/root 目录，运行 RPM 命令进行安装，具体配置命令如下。

```
[root@localhost ~]#rpm –ivh Net-snmp-libs-5.1.2-11
[root@localhost ~]#rpm –ivh net-snmp-5.1.2-11
```

查看软件包是否安装成功。

```
[root@localhost ~]# rpm –qa |grep snmp
net-snmp-libs-5.1.2-11
net-snmp-5.1.2-11
```

2）配置 SNMP 服务

安装好后需要对 mib 支持和 community string（共同体）进行设置，默认 SNMP 主配置文件为/etc/snmp/snmpd.conf，具体配置命令如下。

```
[root@localhost ~]#vi /etc/snmp/snmpd.conf
```

打开配置文件后需要做以下几点配置。

（1）修改 community string。

在配置文件 41 行可以设定默认的 community string 值，将 public 改为更安全的口令。

```
41 Com2sec notConfigUser default public
```

（2）修改管理信息库。

在配置文件 62 行可以修改默认使用的管理信息库，将该行的 systemview 修改为 mib2，并确保 88 行前面的#号去掉。

```
62 Access notConfigGroup any noauth exact s mib2 none none
……
88 View mib2 included .iso.org.dod.internet.mgmt.mib-2 fc
```

（3）重启 SNMP 服务。

配置结束后必须重启服务才可生效。SNMP 程序的服务名为 snmpd，可以使用以下两种方法重启该服务。

```
[root@localhost ~]#/etc/init.d/snmpd testart
```

或

```
[root@localhost ~]#Service snmpd restart
```

3. 开启网络设备的 SNMP 协议

以思科路由器为例配置 SNMP 协议，具体配置命令如下。

```
Router(config)#snmp-server community howin rw
//配置本路由器的读写字串为 howin
Router(config)#snmp-server community howin ro
//配置本路由器的只读字串为 howin
Router(config)#snmp-server enable traps
//允许路由器将所有类型 SNMP Trap 发送出去
Router(config)#snmp-server host IP_SERVER traps howin
//指定路由器 SNMP Trap 的接收者，发送 Trap 时采用 howin 作为字串
Router(config)# snmp-server trap-source loopback0
//将 loopback 接口的 IP 地址作为 SNMP Trap 的发送源地址，注意先配好 IP 地址
```

16.2 安装 SolarWinds 网管工具

SolarWinds 网管工具可以安装在网络中的任何位置，只要可以通过该位置访问到网络中的其他被管设备即可。

安装 SolarWinds 网管工具的具体操作步骤如下。

01 双击 SolarWinds 网管工具的安装程序，弹出 Welcome 对话框，单击 Next 按钮，如图 16-15 所示。

02 弹出 End User License Agreement 对话框，单击 Yes 按钮，如图 16-16 所示。

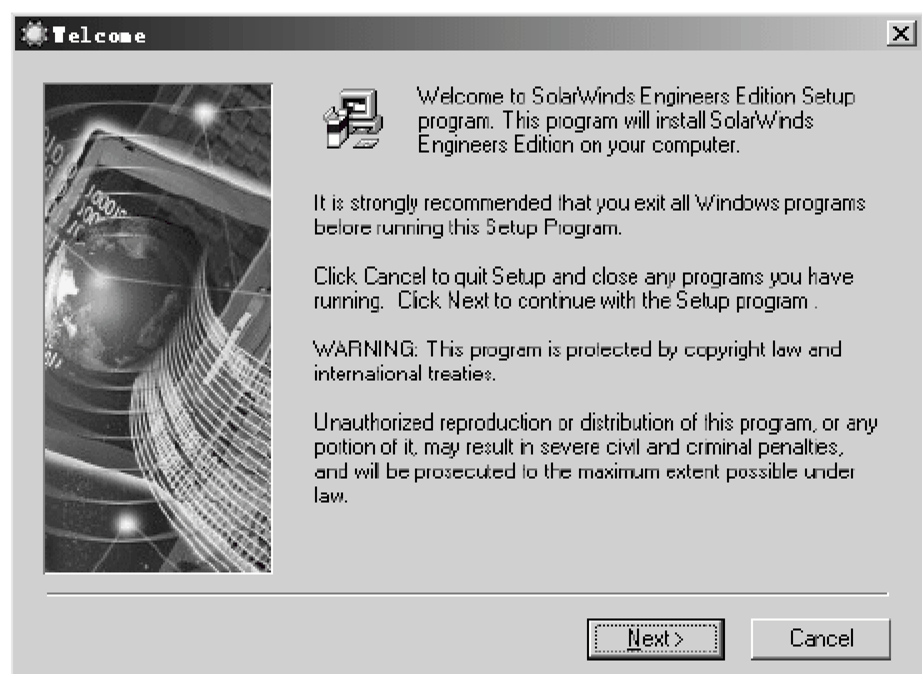


图 16-15 Welcome 对话框

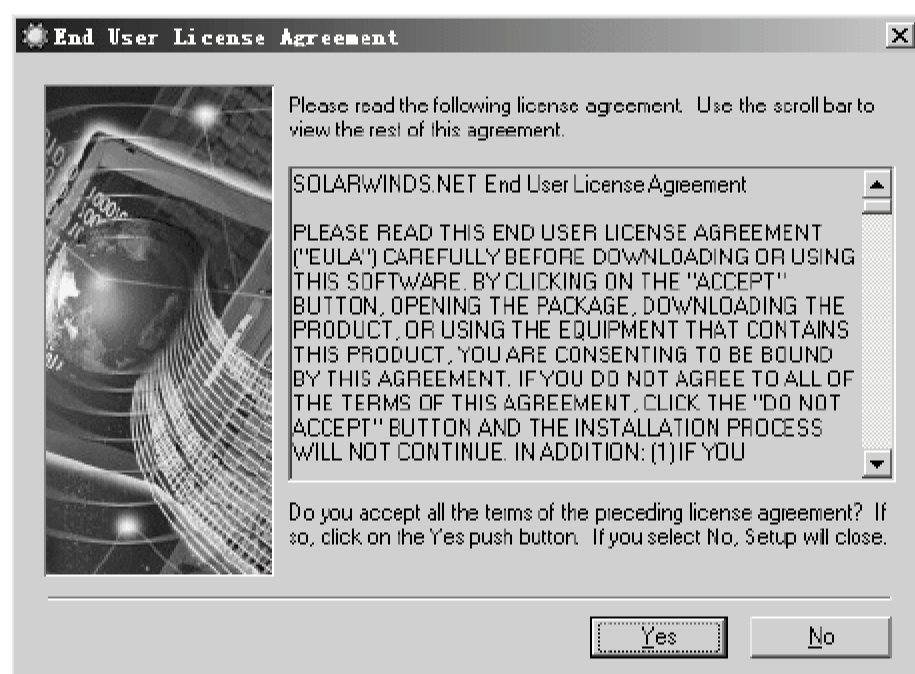


图 16-16 End User License Agreement 对话框

03 弹出 Choose Destination Location 对话框，单击 Browse 按钮可以指定新的安装目录，本实例采用默认值“C:\Progray Files\SolarWinds”，单击 Next 按钮，如图 16-17 所示。

04 弹出 Installing 对话框，系统显示安装进度，如图 16-18 所示。

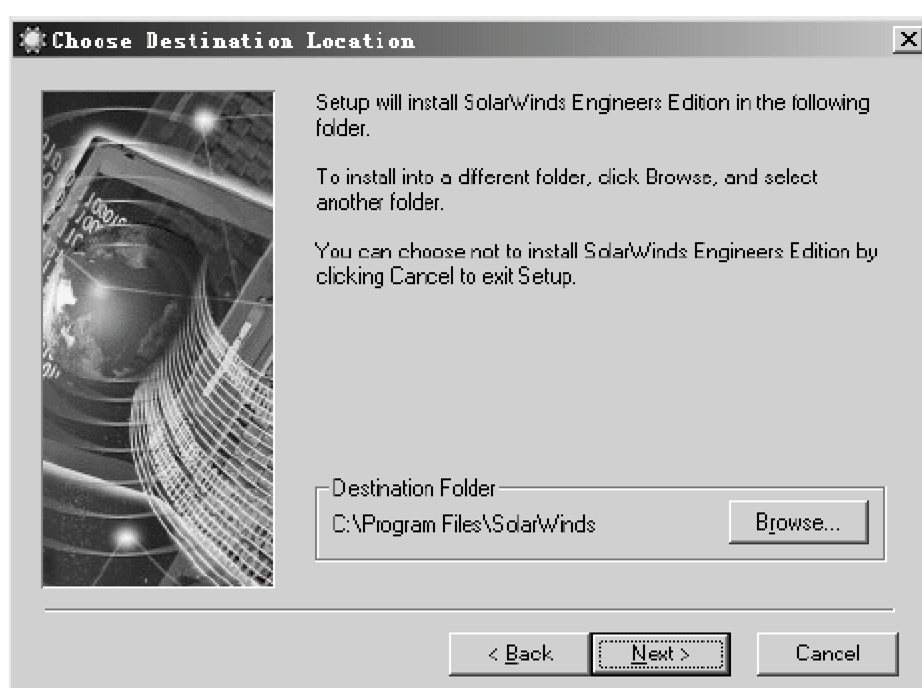


图 16-17 Choose Destination Location 对话框

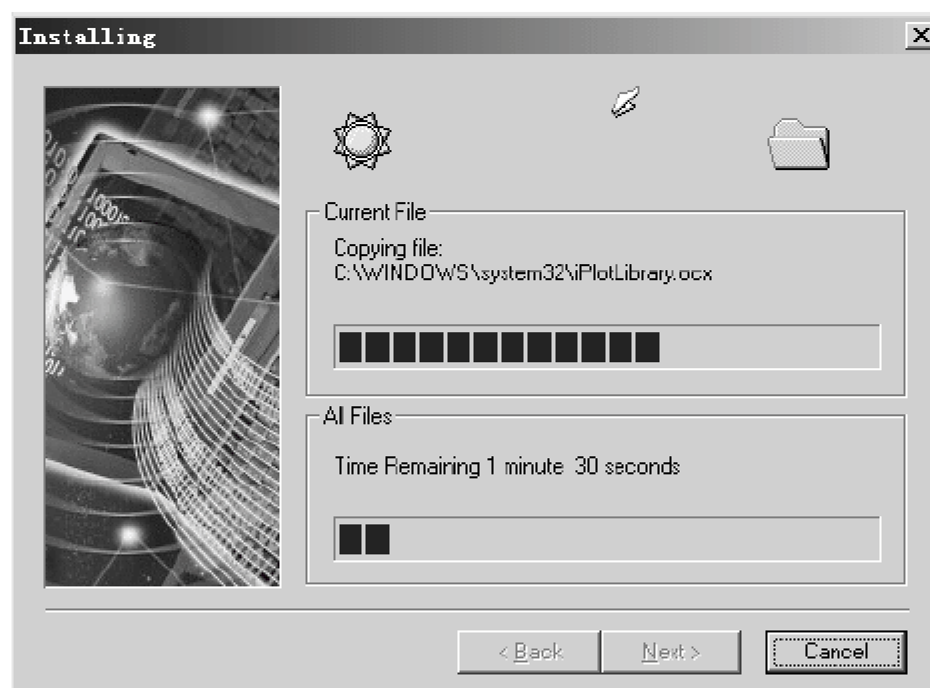


图 16-18 Installing 对话框

05 安装完成，弹出 Installation Complete 对话框，单击 Finish 按钮，如图 16-19 所示。

06 弹出如图 16-20 所示的软件注册对话框，单击 Skip This and Enter Software License Key Now 按钮。



图 16-19　Installation Complete 对话框



图 16-20　软件注册对话框

07 在弹出的对话框的 Enter Software License Key 文本框中输入已获得的许可，单击 Continue 按钮，如图 16-21 所示。

08 弹出新对话框，显示“Your Software License Key is Installed!”（你的软件授权许可已经生效），单击 Continue 按钮，完成 SolarWinds 网管工具的安装，如图 16-22 所示。



图 16-21　输入授权许可对话框



图 16-22　软件授权成功对话框

16.3　项目实战 2：使用 SolarWinds 网管工具

SolarWinds 网管工具可以实现的网络管理功能比较多，下面分别进行介绍。

16.3.1　IP Network Browser

SolarWinds 网管工具安装完成之后会在系统桌面上自动产生 IP Network Browser（IP 网络浏览）工具的快捷方式图标，通过该工具可以查看指定的 IP 子网或主机的信息，不过要查看客户机的设备信息，需要在客户机开启 SNMP 协议。

IP Network Browser 工具的具体使用方法如下。

1. 配置初始化

第一次使用 IP Network Browser 工具需要对其网络连接类型和 SNMP community 作初始配置，具体操作步骤如下。

01 在桌面双击 IP Network Browser 工具的程序图标，弹出 Configuration Wizard 对话框，通过本向导可以进行 IP Network Browser 工具的初始化配置，单击 Cancel 按钮可以关闭配置向导，本实例单击 Next 按钮，如图 16-23 所示。

02 如图 16-24 所示，在弹出的新对话框中可以设定网管工具查看信息所使用的 SNMP community（共同体名），默认值为“public”，可以在 Add 文本框中输入新的 SNMP community，并单击 Add 按钮确认。选择有效的 SNMP community 后，单击 Next 按钮。

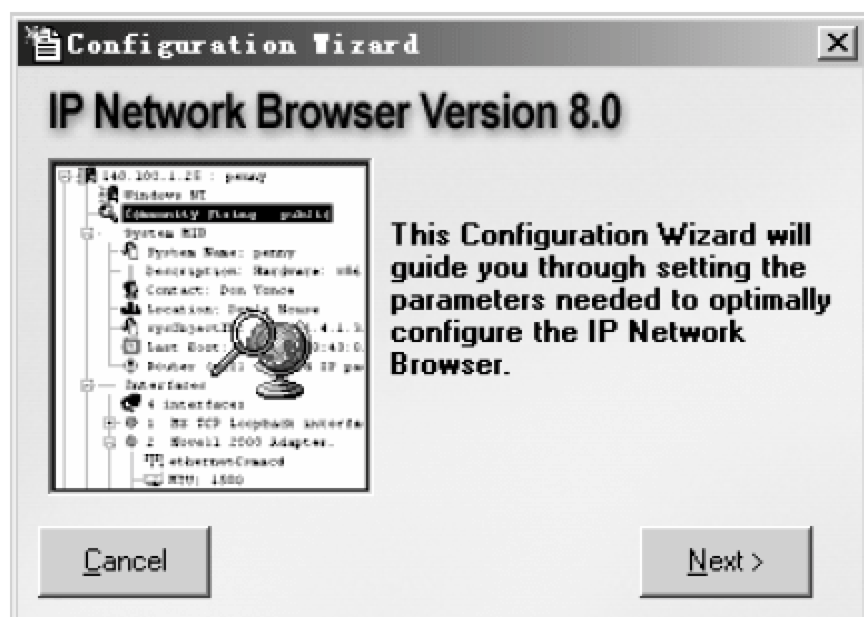


图 16-23 Configuration Wizard 对话框

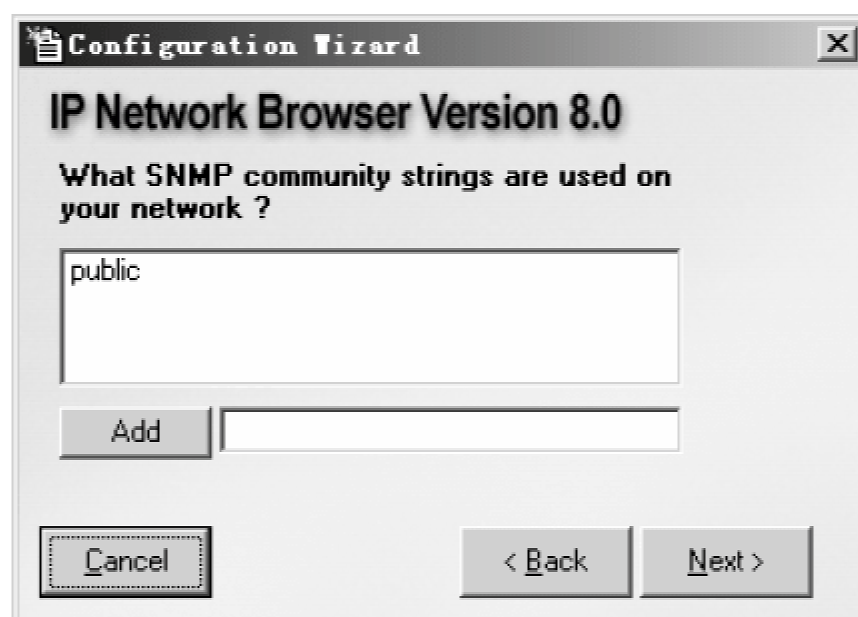


图 16-24 SNMP community 配置对话框

03 如图 16-25 所示，在弹出的新对话框中选择网络连接方式，“Dial-up”代表拨号连接的网络，一般选中 Direct connection to a LAN（直连一个局域网）单选按钮，单击 Next 按钮。

04 配置向导配置结束，弹出如图 16-26 所示的对话框，单击 Finished 按钮。

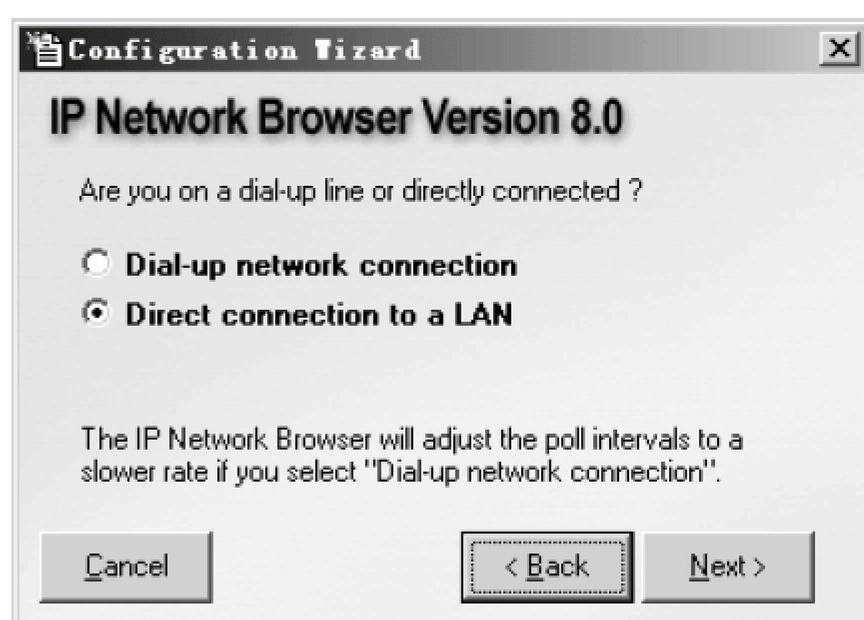


图 16-25 选择网络连接方式



图 16-26 配置向导配置完成

2. 扫描目标网络信息

使用 IP Network Browser 网管工具可以对单个主机、子网、地址区间进行扫描，下面详细讲解扫描目标主机以及查看其信息的方法。

1）扫描单个主机信息

扫描单个主机信息的具体操作步骤如下。

01 打开 IP Network Browser 工具界面，在 Scan a Single Device（扫描单个设备）选项域的 Hostname or IP Address（主机名或 IP 地址）文本框中输入目标主机的 IP 地址，本实例扫描主机“192.168.1.102”，单击 Scan Device 按钮，如图 16-27 所示。

02 扫描结束，如图 16-28 所示，主机“192.168.1.102”的信息已经获得。目标主机 192.168.1.102 的主机名为 SERVER2，是“Windows 2003 Server”操作系统，扫描信息使用的 Community String 为 public。

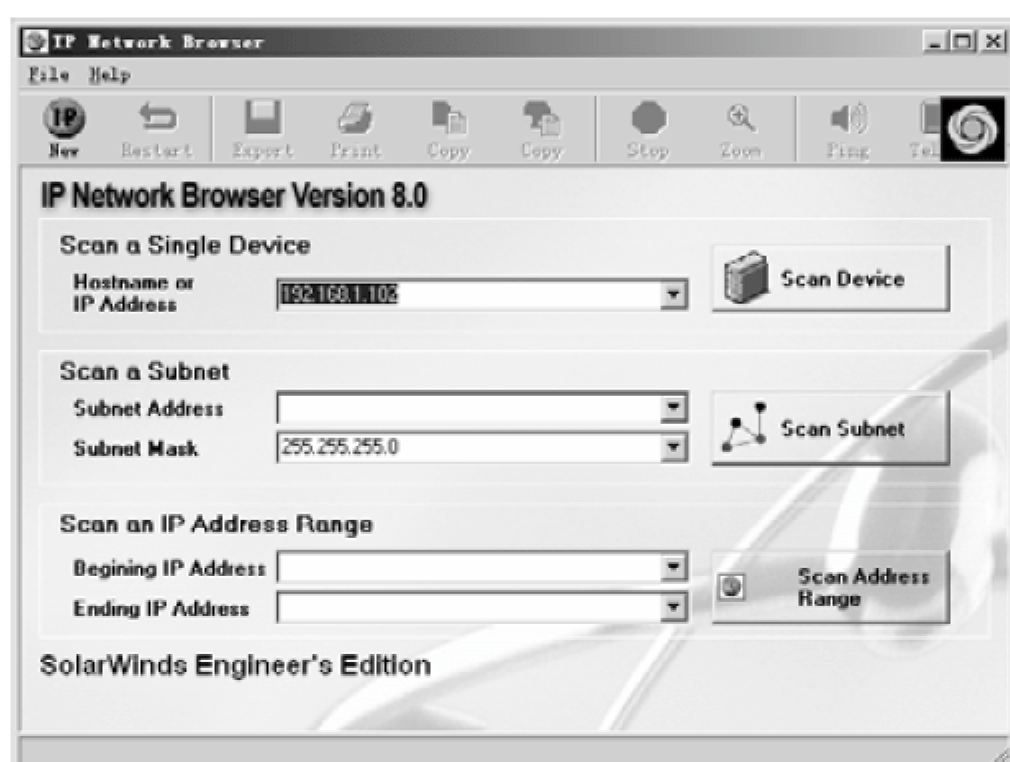


图 16-27 IP Network Browser 窗口

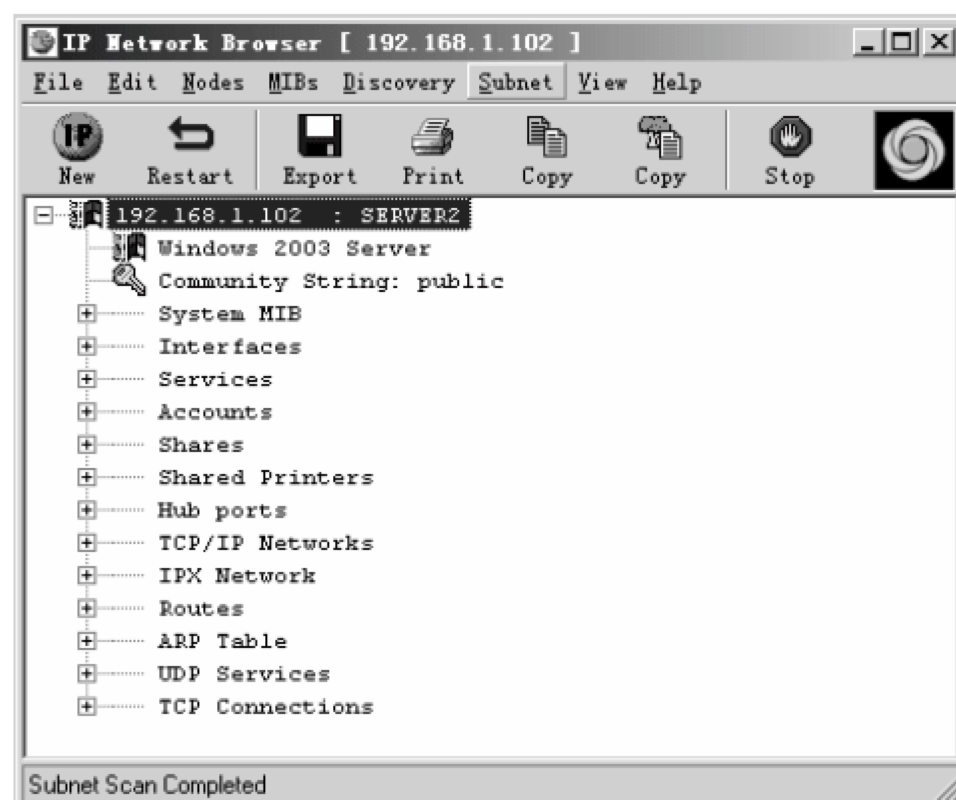


图 16-28 主机 192.168.1.102 的扫描结果

03 选择 System MIB（系统管理信息库）选项，如图 16-29 所示，显示了目标主机支持的 MIB 库 ID 等信息。

04 选择 Interfaces 选项，如图 16-30 所示，显示目标主机的接口数量，一共有两个接口，并分别显示接口的详细信息。

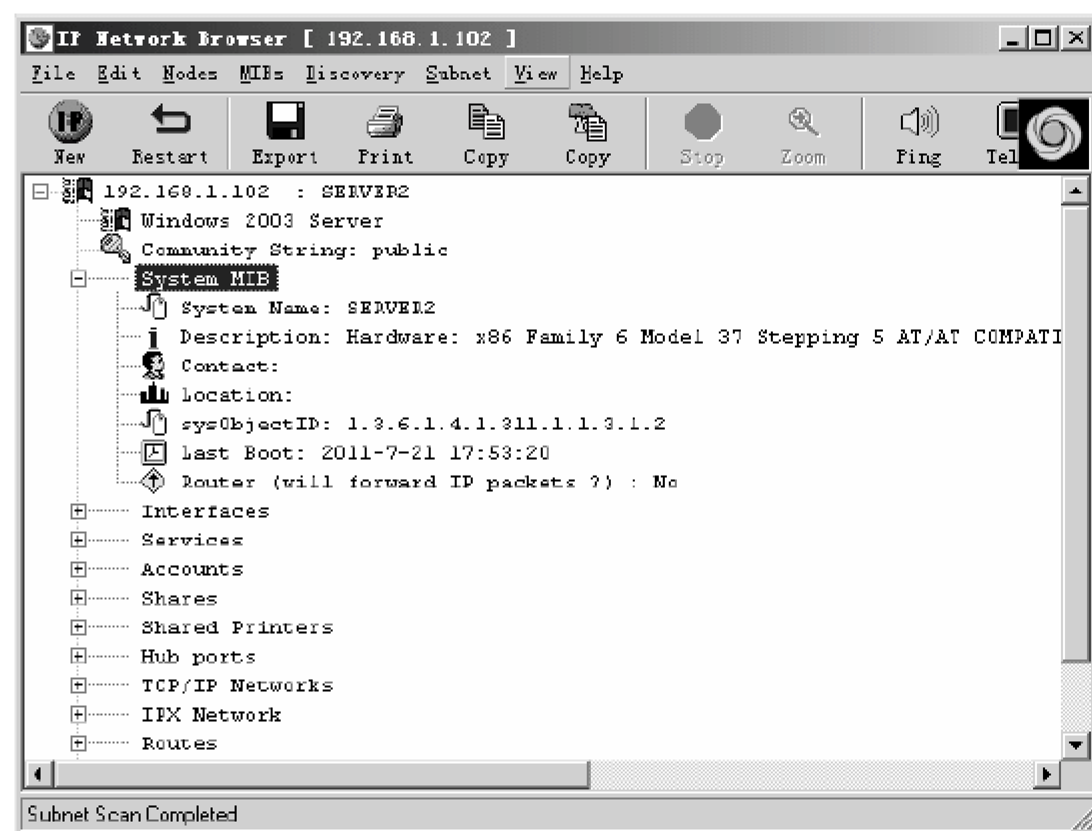


图 16-29 目标主机的 System MIB 信息

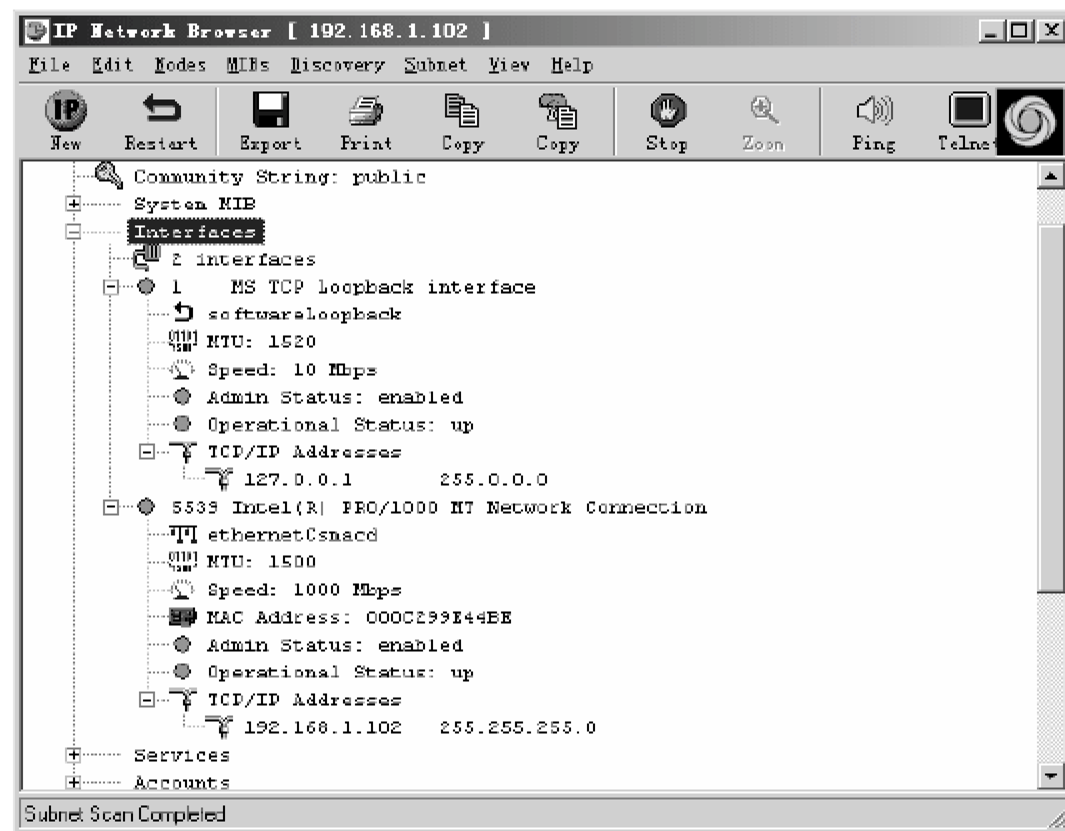


图 16-30 目标主机的 Interfaces 信息

接口信息介绍如下。

- softwareLoopback：表示该接口为软件回环接口。
- ethernetCsmacd：满足 CSMA/CD 的以太网接口，CSMA/CD 是带有冲突检测的载波侦听多路访问。

- MTU：最大传输单元。
- Speed：接口带宽。
- MAC Address：物理网卡地址。
- TCP/IP Address：IP 地址。

05 选择 Services 选项，如图 16-31 所示，显示目标主机已经开启的服务。过多的无必要的服务项可以影响服务器整体性能，所以在管理服务器时，服务项是重要的管理内容之一。

06 选择 Accounts 选项，如图 16-32 所示，显示目标主机的系统账户信息。

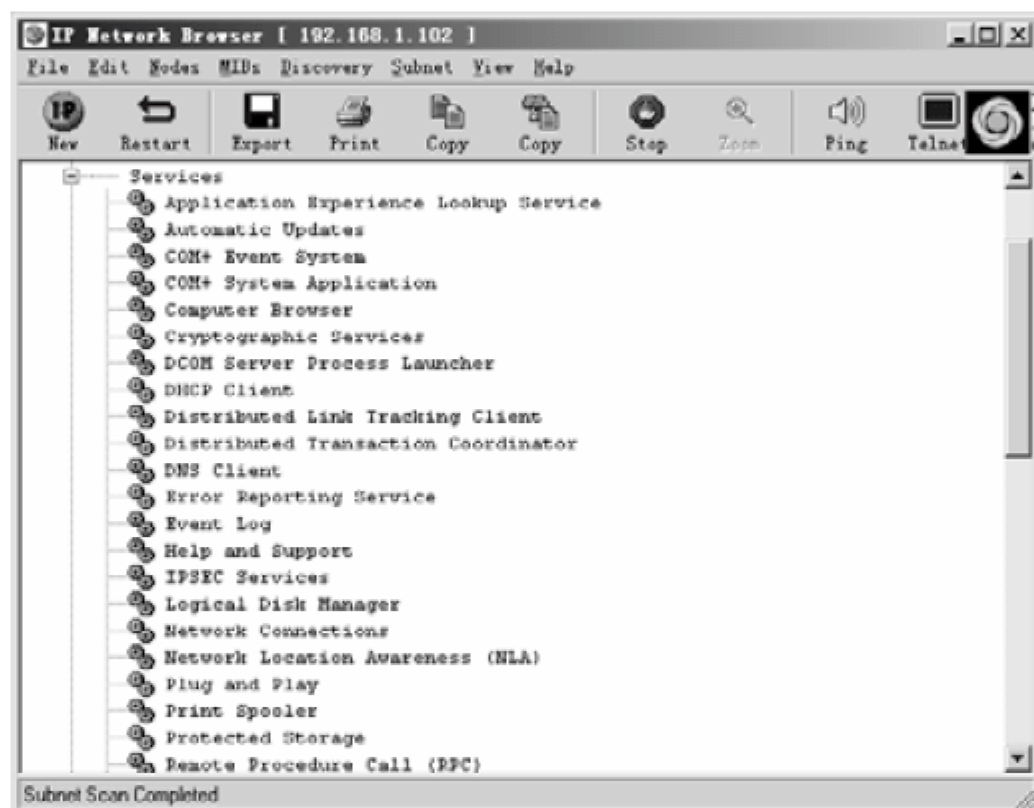


图 16-31　目标主机的 Services 信息

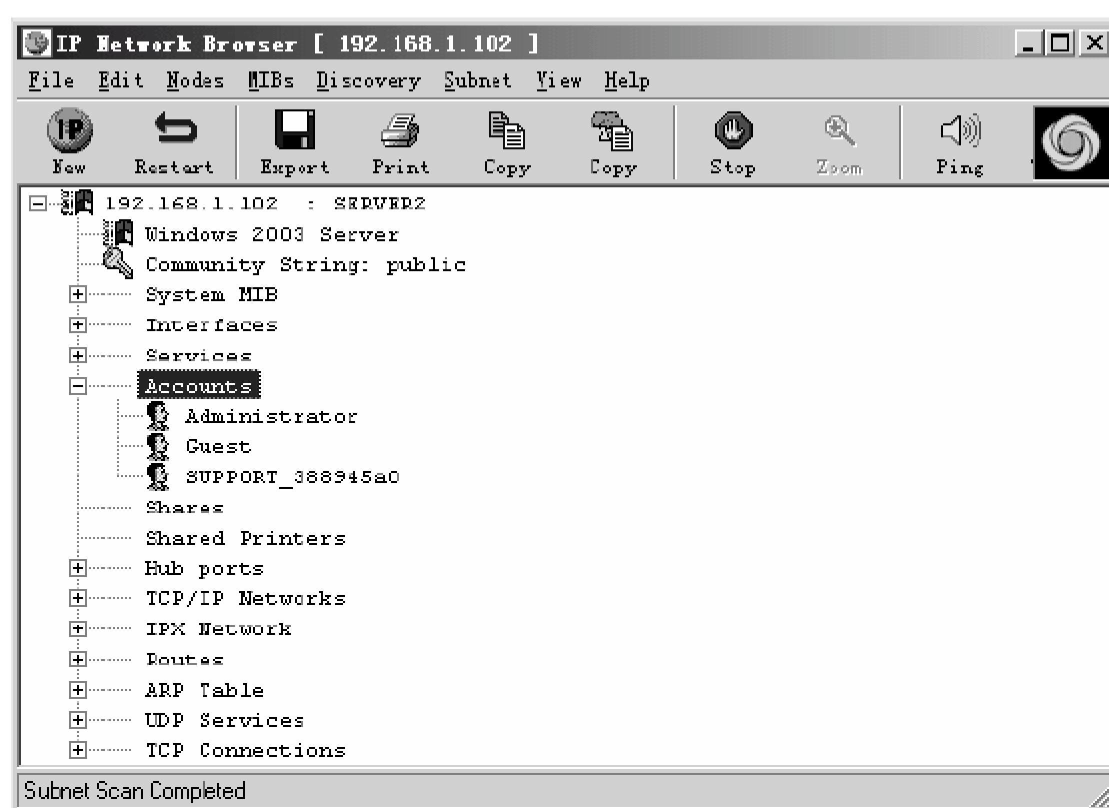


图 16-32　目标主机的 Accounts 信息



提 示

Shares 和 Shares Printers 两项内容目标主机没有配置，所以无信息显示。

07 选择 TCP/IP Networks 选项，如图 16-33 所示，显示目标主机的网络地址信息，目标主机有两个 IP 地址，“127.0.0.1”回环地址和“192.168.1.102”物理网卡地址。

08 选择 Routes 选项，如图 16-34 所示，显示目标主机的路由表信息，包括 Next Hop 和 Last Updated 等内容。

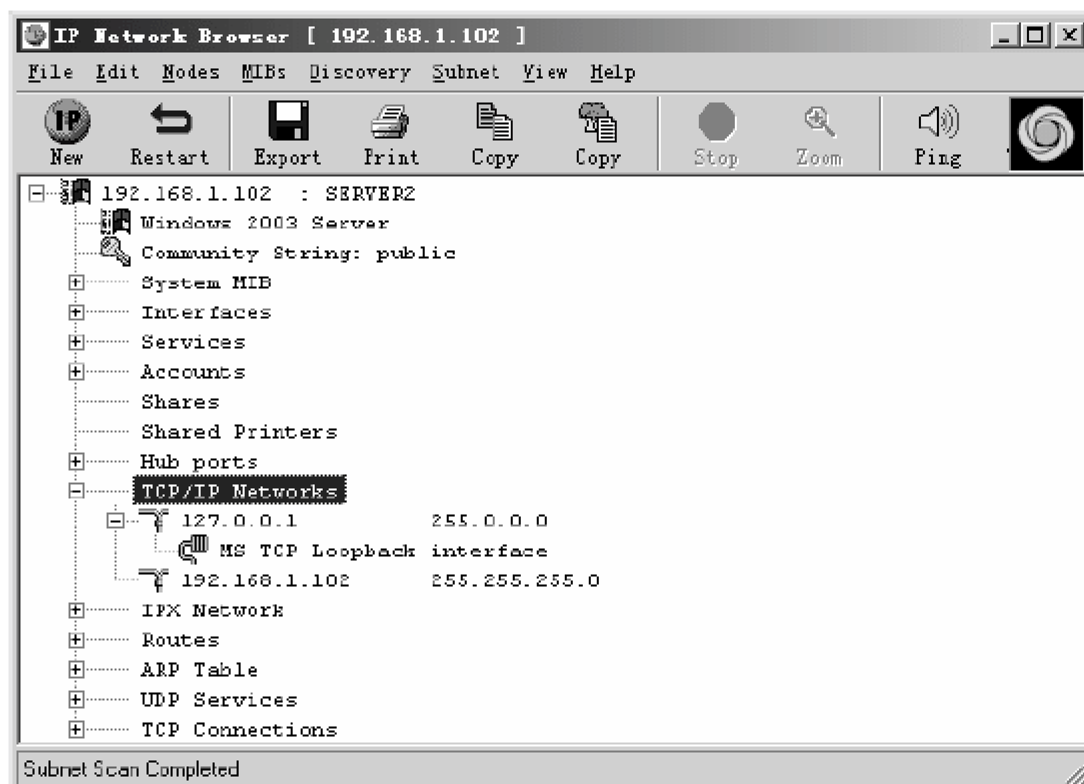


图 16-33　目标主机的 TCP/IP Networks 信息

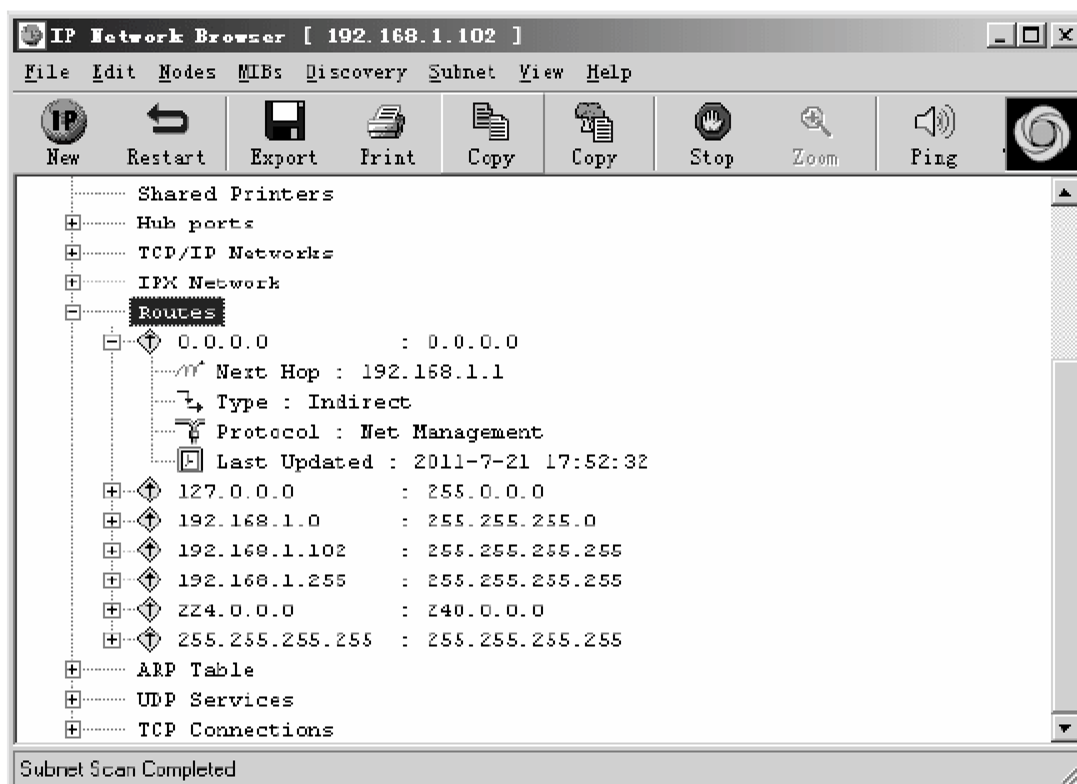


图 16-34　目标主机的 Routes 信息

09 选择 ARP Table 选项，如图 16-35 所示，显示目标主机记录的 ARP 对应关系表和学习的 MAC 地址表。

10 选择 UDP Services 和 TCP Services 选项，如图 16-36 所示，分别显示目标主机已开通的端口及对应的服务程序，可用于发现目标主机的端口漏洞。

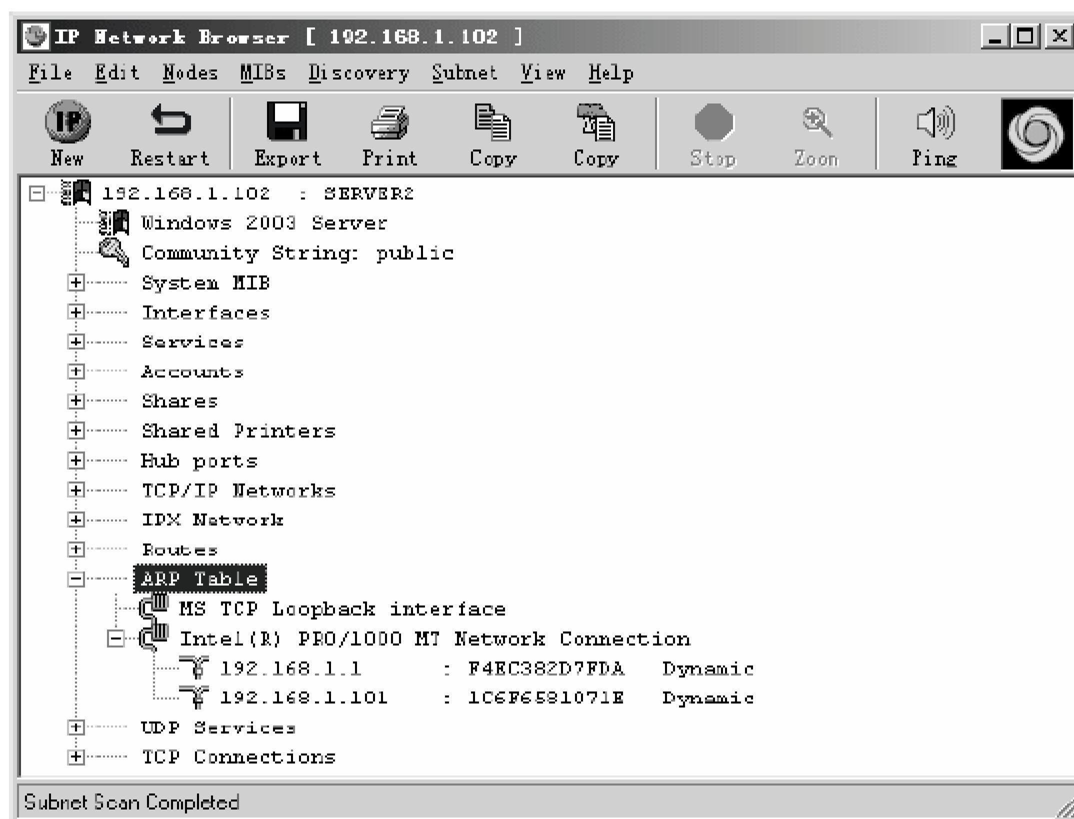


图 16-35　目标主机的 ARP Table 信息

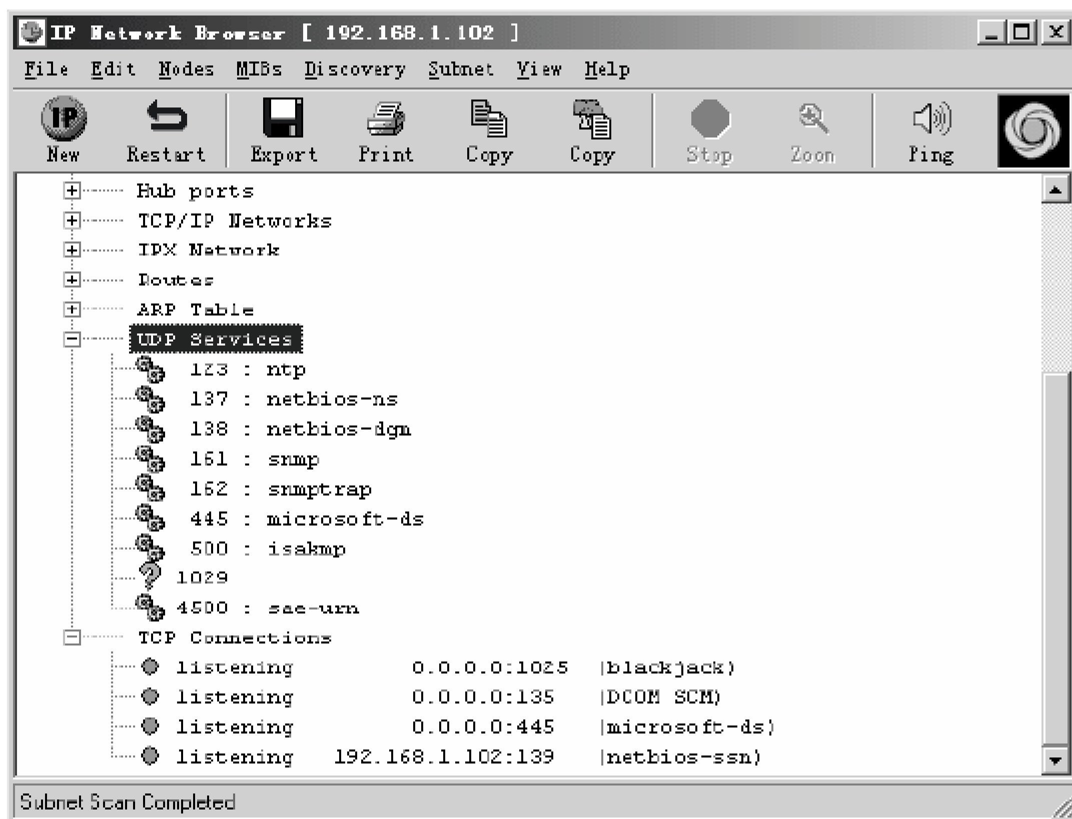


图 16-36　目标主机的 UDP 和 TCP 已用端口信息

2）扫描目标子网主机信息

扫描目标子网主机信息的具体操作步骤如下。

01 打开 IP Network Browser 工具界面，在 Scan a Subnet（扫描一个子网）选项域的 Subnet Address（子网地址）和 Subnet Mask（子网掩码）文本框中分别输入目标子网地址及掩码，本实例扫描子网“192.168.1.0”，掩码“255.255.255.0”，单击 Scan Subnet（扫描子网）按钮，如图 16-37 所示。

02 扫描结束，如图 16-38 所示，在子网“192.168.1.0/24”中共扫描到 6 台主机，其中“192.168.1.10”和“192.168.1.20”主机前显示 Cisco 图标，并在后方显示设备名为“R1”和“R2”，在“192.168.1.102”前显示微软窗口图标，表示为 Windows 系统，并显示设备名为“SERVER2”。扫描到的其他三台设备没有信息设备信息显示，主要是因为其没有配置 SNMP 或者 SNMP 服务的 community（共同体）配置不匹配。

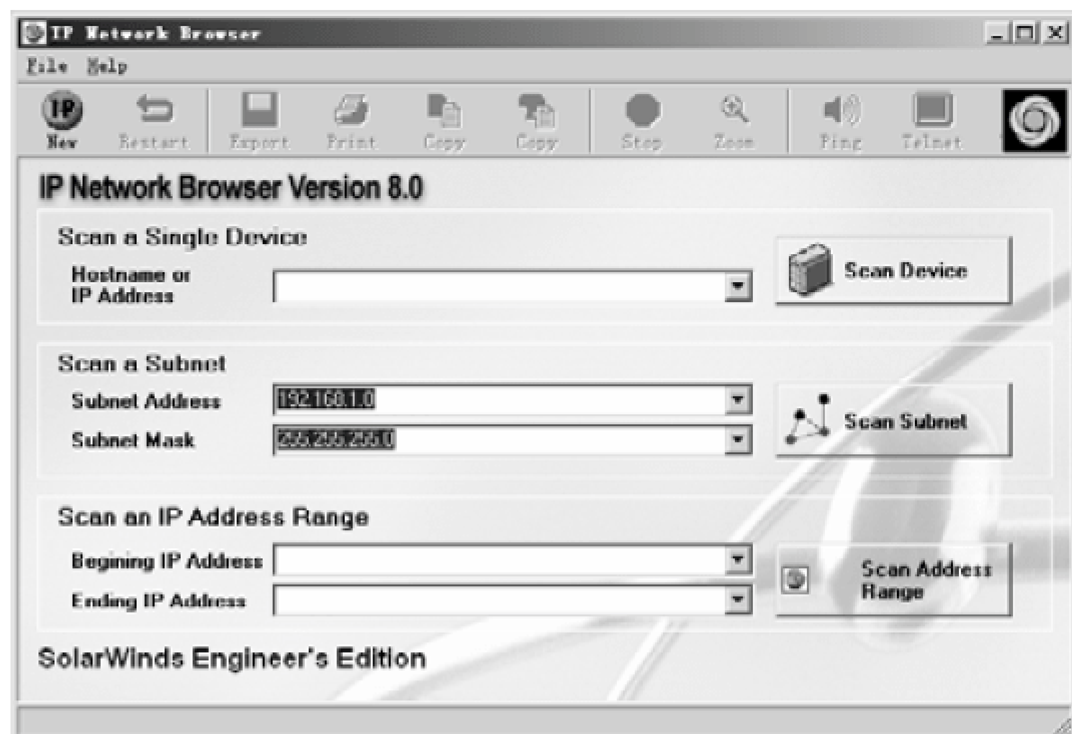


图 16-37　IP Network Browser 窗口

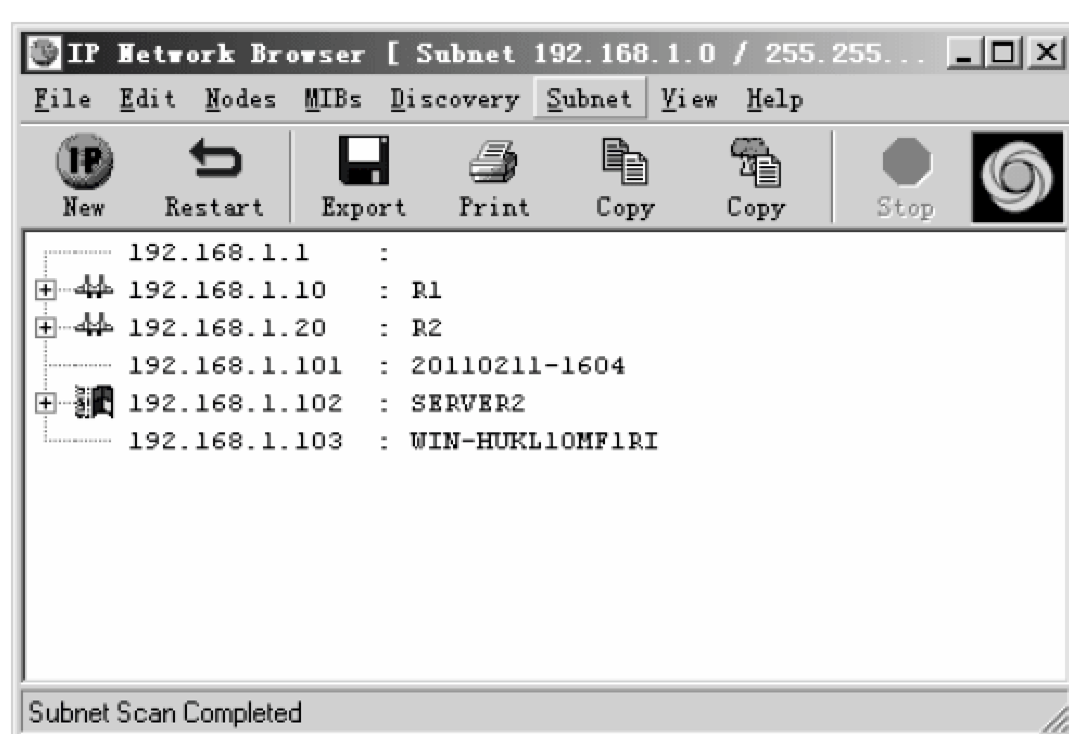


图 16-38　子网 192.168.1.0/24 的扫描结果

03 展开设备 192.168.1.10 的搜索结果，如图 16-39 所示，显示当前设备为 Cisco 7206 系列及其他信息。

04 展开设备 192.168.1.10 的 IOS 信息，如图 16-40 所示，显示该设备的系统镜像信息。

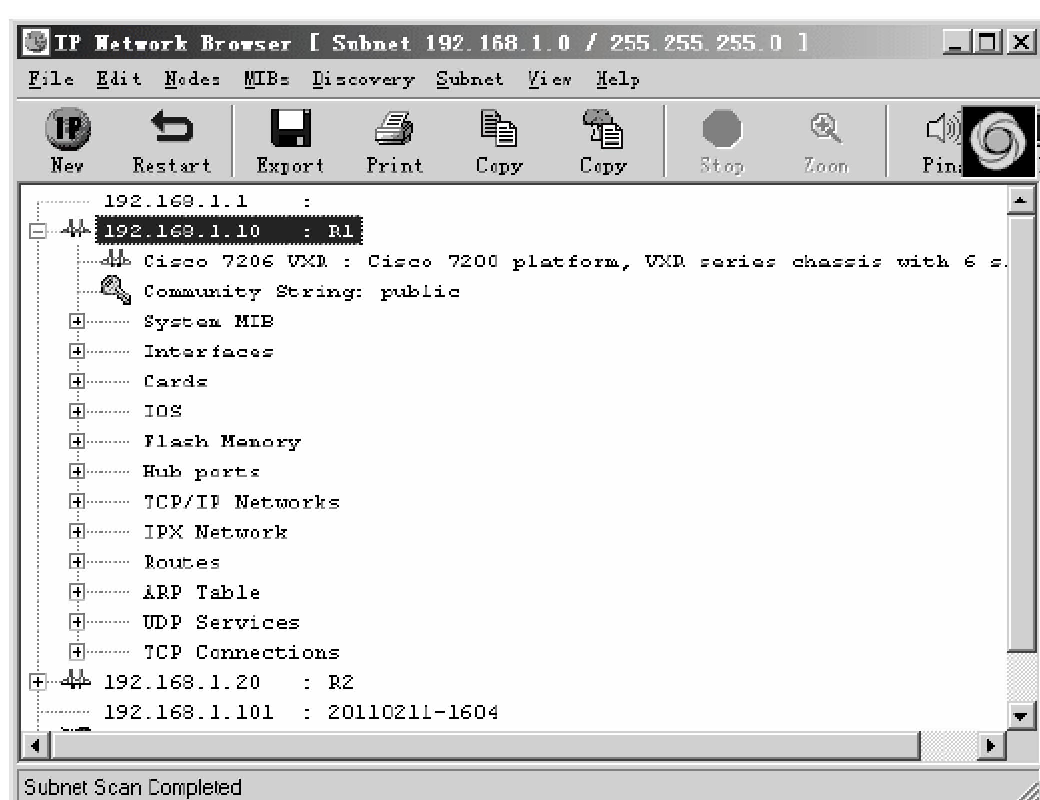


图 16-39　目标设备的管理信息

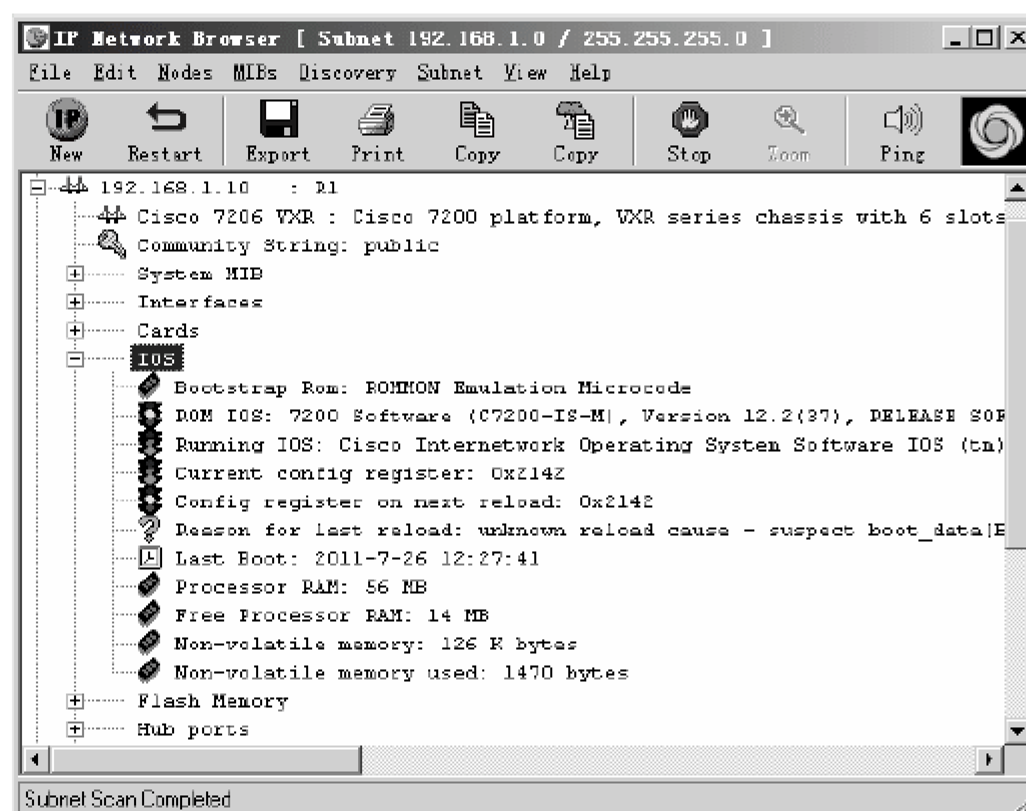


图 16-40　目标设备的 IOS 镜像信息

设备 IOS 镜像信息介绍如下。

- Bootstrap Rom：初始引导程序存储器型号。
- ROM IOS：表示 ROM 芯片中的 IOS 镜像版本。
- Running IOS：正在运行的 IOS 镜像。
- Current config register：当前寄存器的值，0x2142 表示启动设备时不加载 startup-config 配置文件。
- Config register on next reload：配置的下次重启后寄存器的值。
- Processor RAM：处理器缓存空间。
- Non-volatile memory：可用内存空间。



提 示

设备的其他信息上文中已经做了介绍，读者需要注意的是，应当提高实际需求中对有价值信息的查找效率。

3. 附加测试工具

在 IP Network Browser 工具中还附加了一些小工具，包括 Ping、Telnet、Trace 等。以 Ping 为例，使用方法介绍如下。

01 选择需要使用 ping 命令的设备，如图 16-41 所示，单击工具栏中的 Ping 按钮。

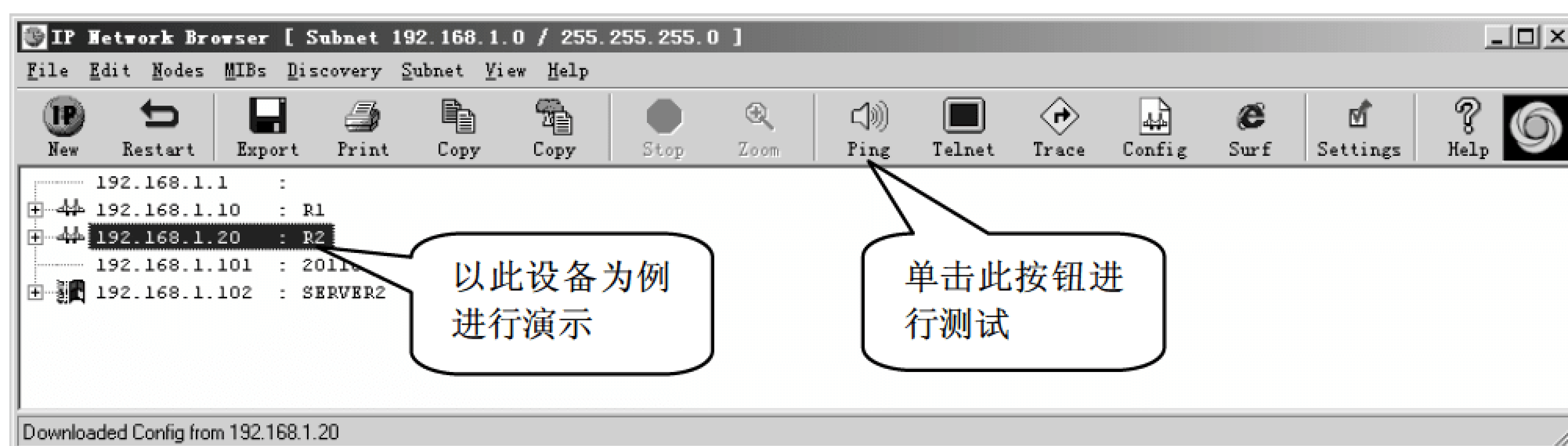


图 16-41　对设备 192.168.1.20 进行 Ping 操作

02 Ping 测试结束，显示测试结果，如图 16-42 所示，设备 192.168.1.20 在 3μs 内作出请求回应。

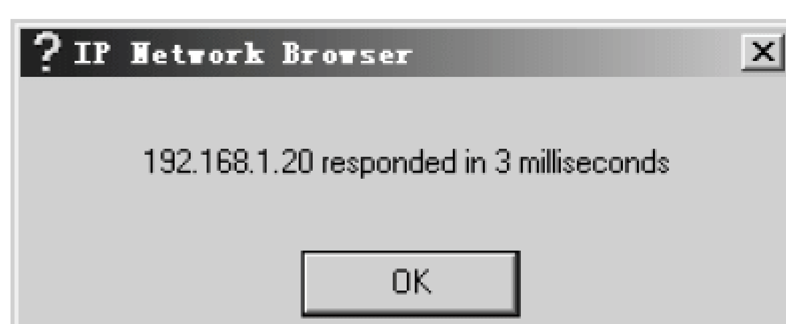


图 16-42　Ping 测试结果

16.3.2　Network Performance Monitor

SolarWinds 网管工具安装完成之后会在系统桌面上自动产生 Network Performance Monitor（网络性能监视）工具的快捷方式图标，通过该工具可以查看目标设备的性能信息。

Network Performance Monitor 工具的具体使用方法如下。

01 双击桌面 Network Performance Monitor 工具快捷方式图标，弹出 Network Performance Monitor（网络性能监视）提示框，单击 Close 按钮，如图 16-43 所示。

02 弹出 Network Performance Monitor 程序窗口，单击工具栏 New 按钮，如图 16-44 所示。

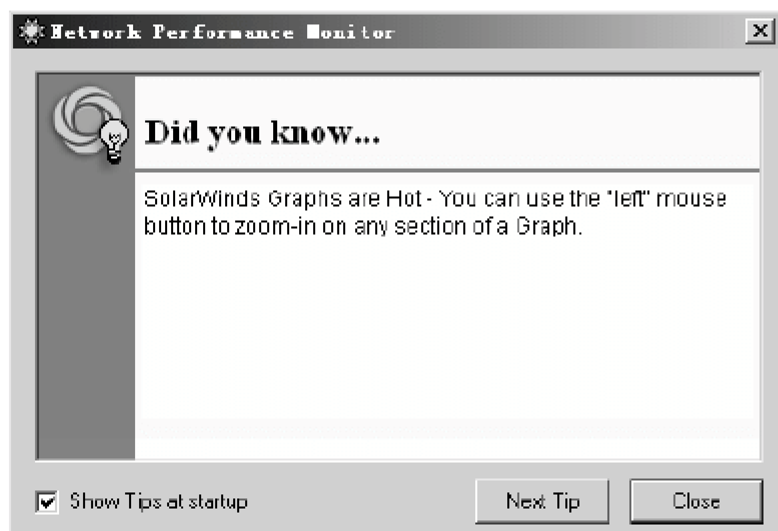


图 16-43　Network Performance Monitor

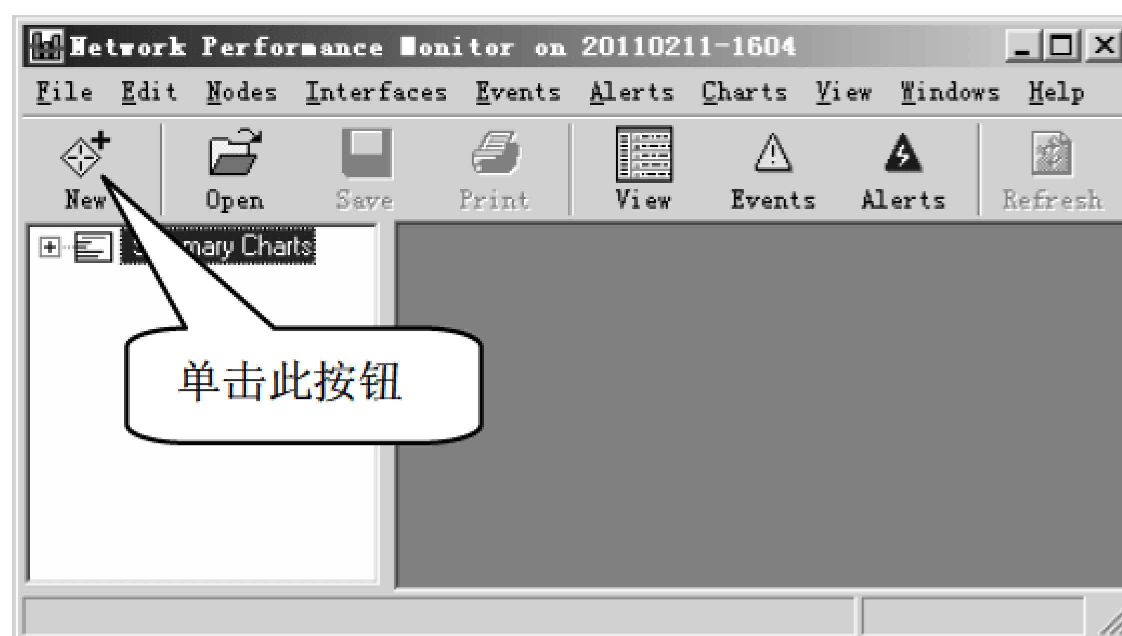


图 16-44　Network Performance Monitor 程序窗口

03 弹出 Add Node or Interface to Monitor（添加节点或接口进行监视）对话框，在【Hostname or IP Address of Server,Router,etc.】（服务器、路由器等的主机名或 IP 地址）对话框中输入需要监控的目标主机地址，本实例采用主机“192.168.1.102”，在 SNMP Community String（SNMP 共同体）文本框中输入有效的共同体名，本实例采用“public”，单击 OK 是按钮，如图 16-45 所示。

04 弹出 Resources on SERVER2server2（主机资源）窗口，此窗口显示了目标主机“SERVER2”可以被监视资源。可通过窗口右侧的功能按钮快速选择需要监控的性能选项，选择完成后单击 OK 按钮，如图 16-46 所示。

功能按钮介绍如下。

- Select All：选择所有选项。
- Deselect All：清除所有选项。
- Select All Volumes：选择所有卷及所有磁盘分区。
- Select All Interfaces：选择所有接口。
- Select All Active Interfaces：选择所有活动接口。

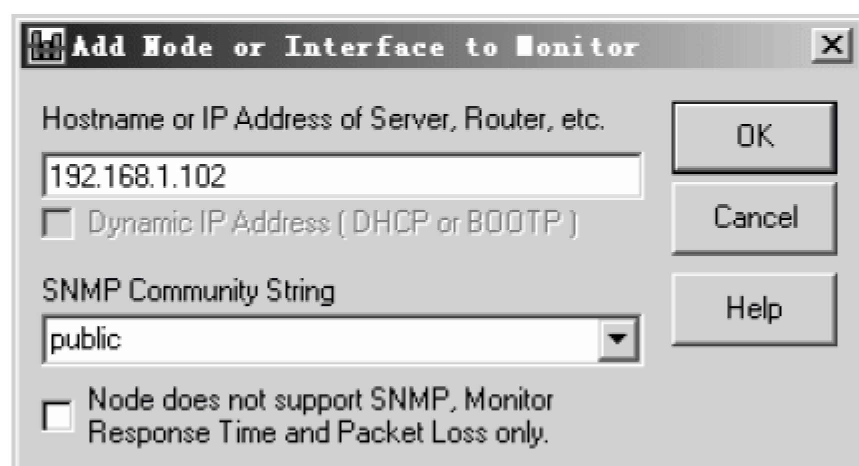


图 16-45　Add Node or Interface to Monitor

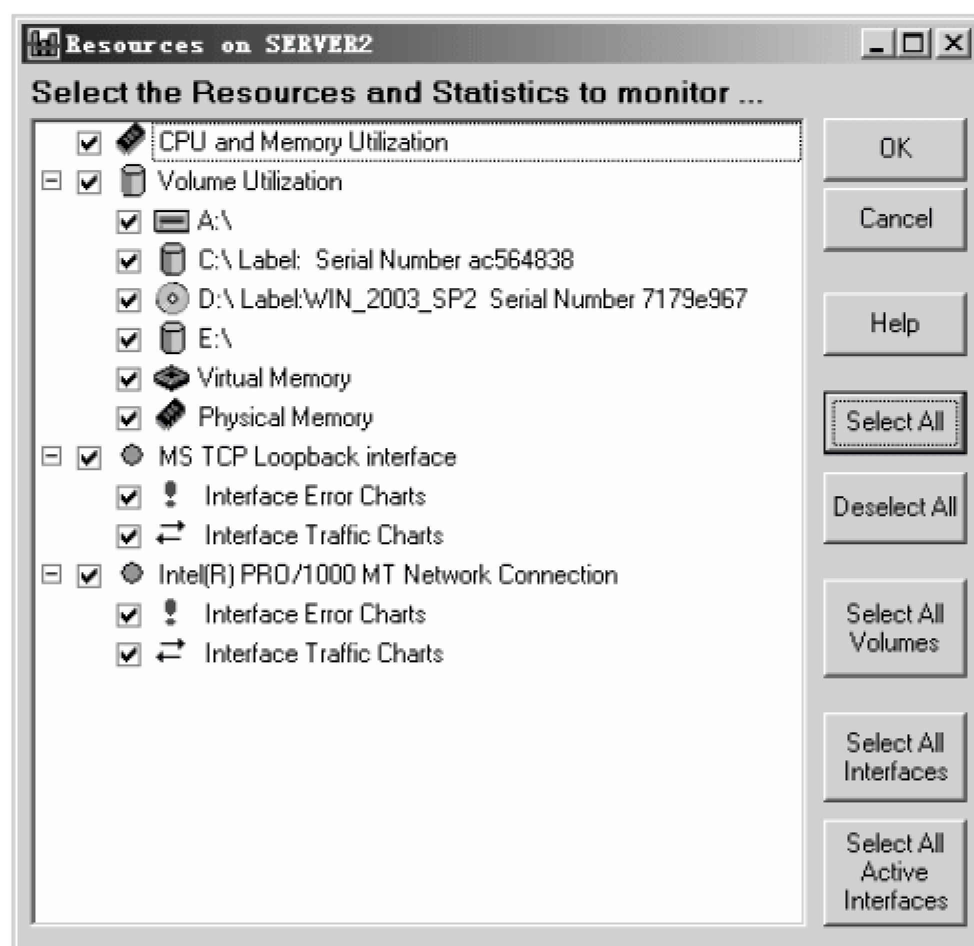


图 16-46　Resources on SERVER2 窗口

05 返回 Network Performance Monitor 窗口，显示了 SERVER2 主机可监视的性能选项，如图 16-47 所示。

06 打开 SERVER2 ➢ CPU Load and Memory Use（CPU 负荷和内存使用）选项列表，可以通过 5 种表查看 CPU 和内存的使用情况，如图 16-48 所示。

表功能介绍如下。

- Average CPU Load：CPU 平均负载。
- Min/Max Average CPU Load：CPU 最小、最大平均负载。
- Average Memory Usage：内存平均使用率。
- Percent Memory Used：内存使用百分比。
- Min/Max Average Memory Usage：内存最小、最大平均使用率。

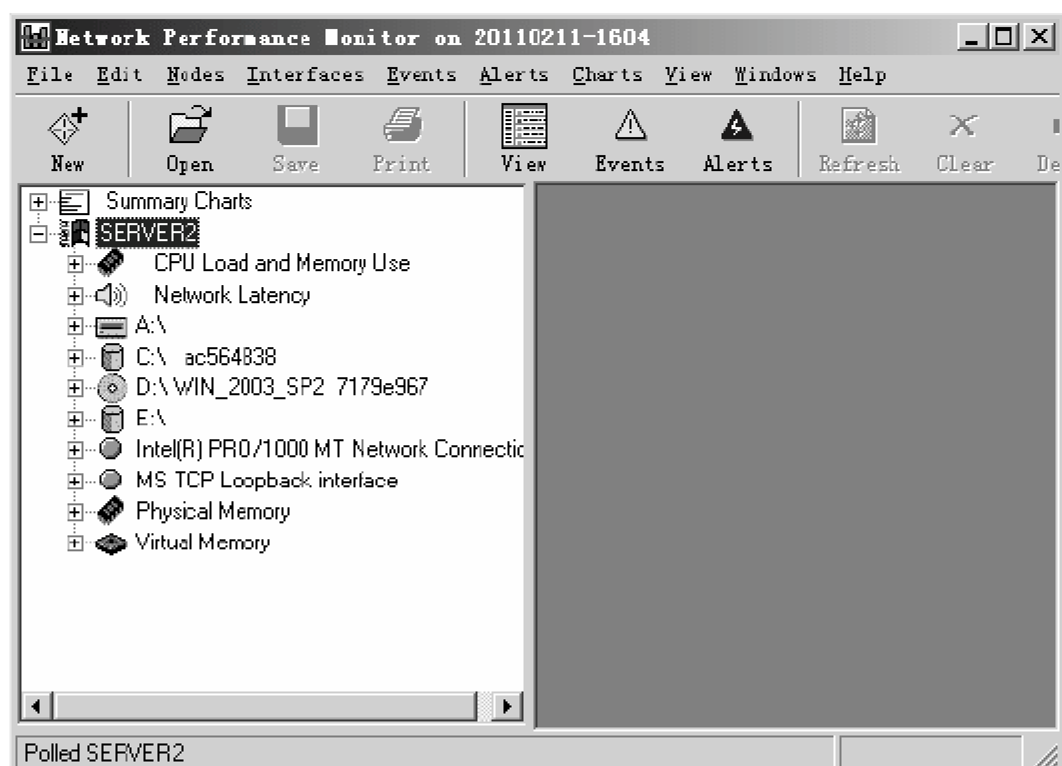


图 16-47　Network Performance Monitor 程序窗口

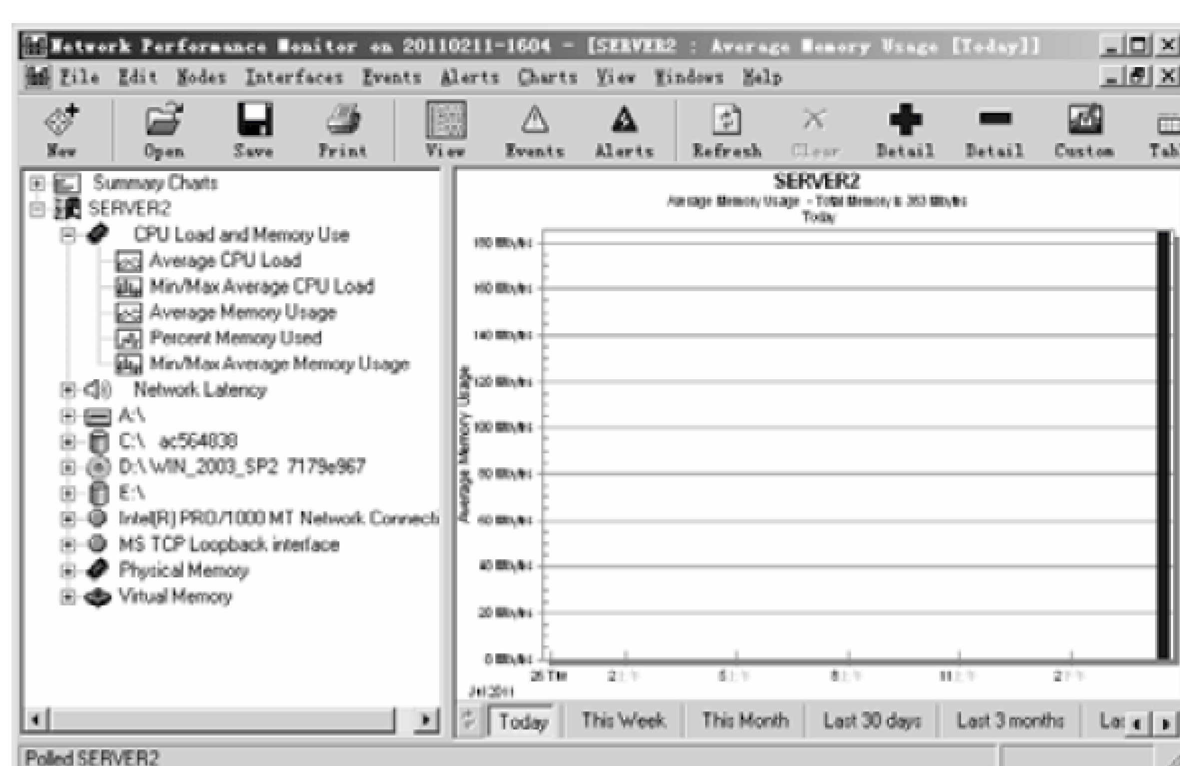


图 16-48　CPU Load and Memory Use 选项列表

07 打开 SERVER2 ➢ Network Latency 网络延迟选项列表，可以通过 9 种表查看网络延迟状况，如图 16-49 所示。

常用表功能介绍如下。

- Average Response Time：平均响应时间。
- Average Response Time & Packet：平均响应时间及数据包。
- Percent Loss – Bat Chart：条线图显示丢包百分比。
- Percent Loss - Line Chart：线形图显示丢包百分比。
- Availability and Response Time：可用性和响应时间。

08 打开 SERVER2 ➢【A:\】选项列表，可以通过 4 种表查看磁盘 A 的使用情况，如图 16-50 所示。

常用表功能介绍如下。

- Min/Max/Average Disk Usage：最小、最大、平均磁盘使用量。
- Percent Disk Usage：磁盘使用百分比。
- Allocation Failures：配置失败记录。
- Volume Size：容量大小。

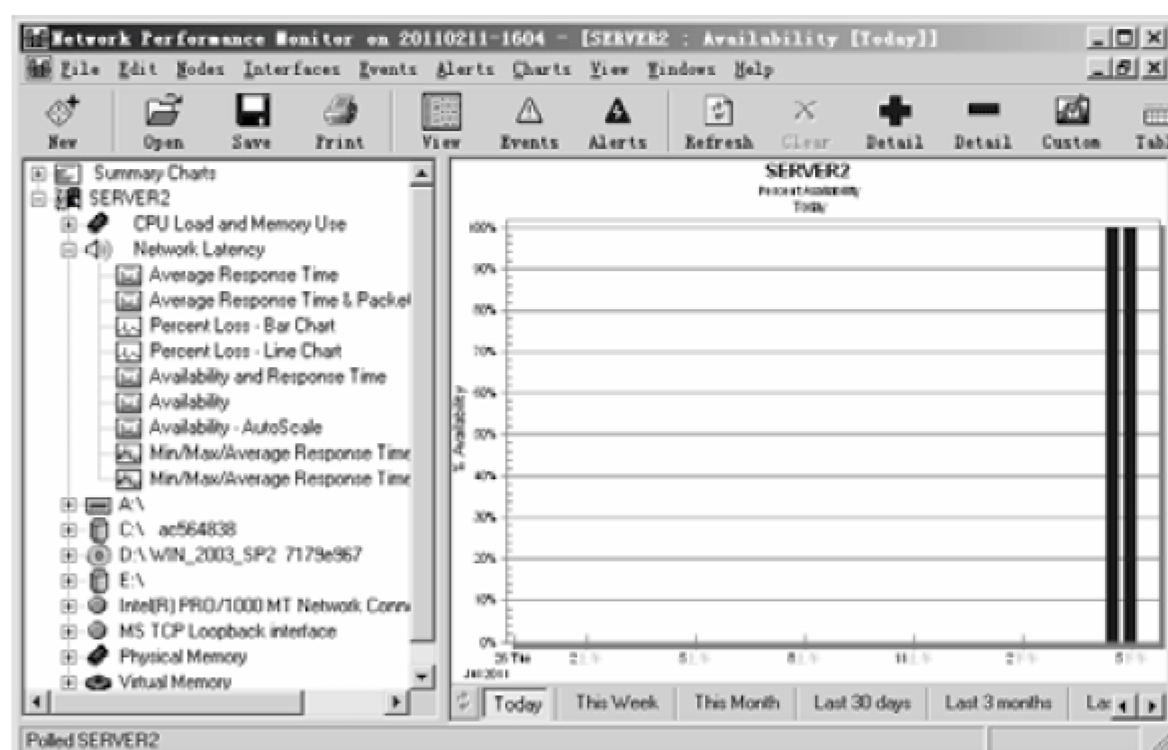


图 16-49　Network Latency 选项列表

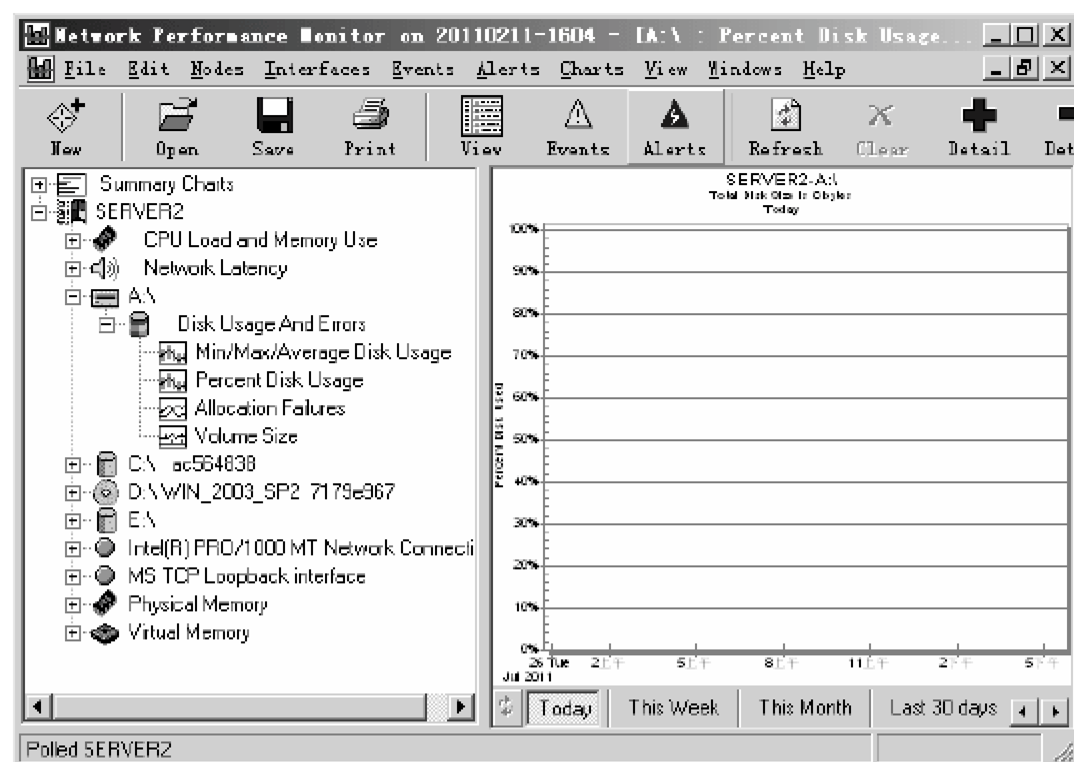


图 16-50　磁盘性能列表

09 打开 SERVER2 ➢ Intel(R)PR0/1000MT Network Connection 选项列表，可以通过多种表查看网卡连接性能，如图 16-51 所示。

10 打开 SERVER2 ➢ Physical Memory（物理内存）选项列表，可以通过 4 种表查看物理内存性能，如图 16-52 所示。

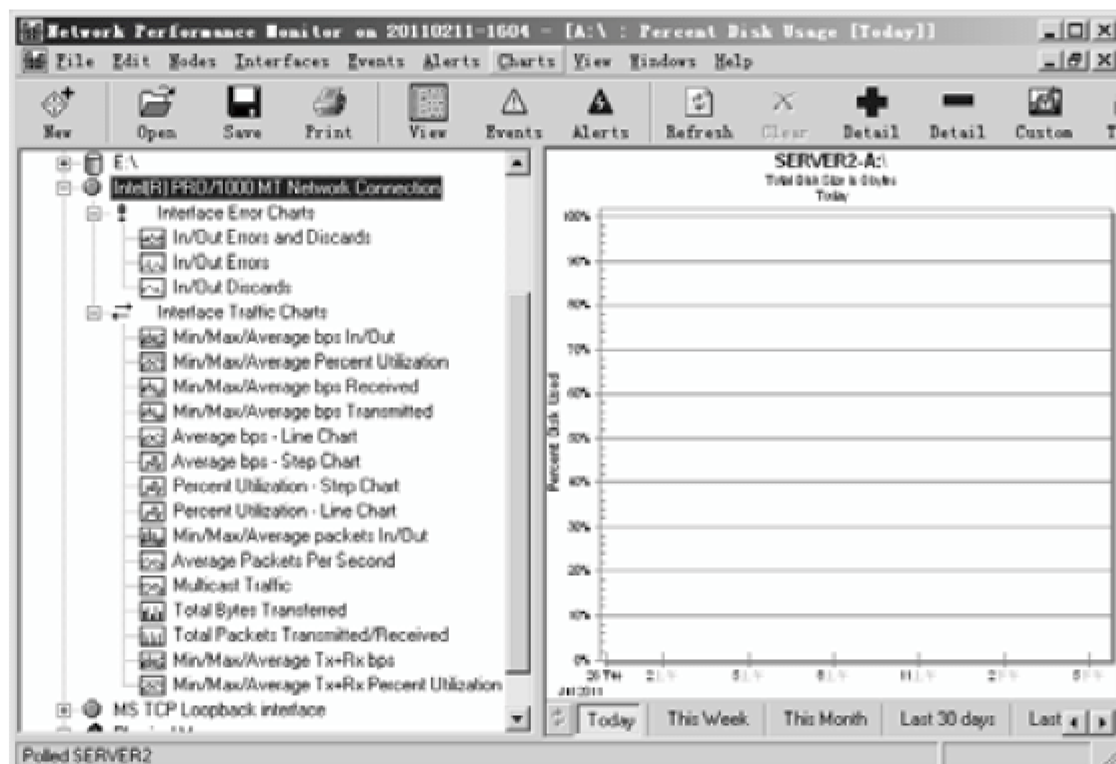


图 16-51 Network Connection 选项列表

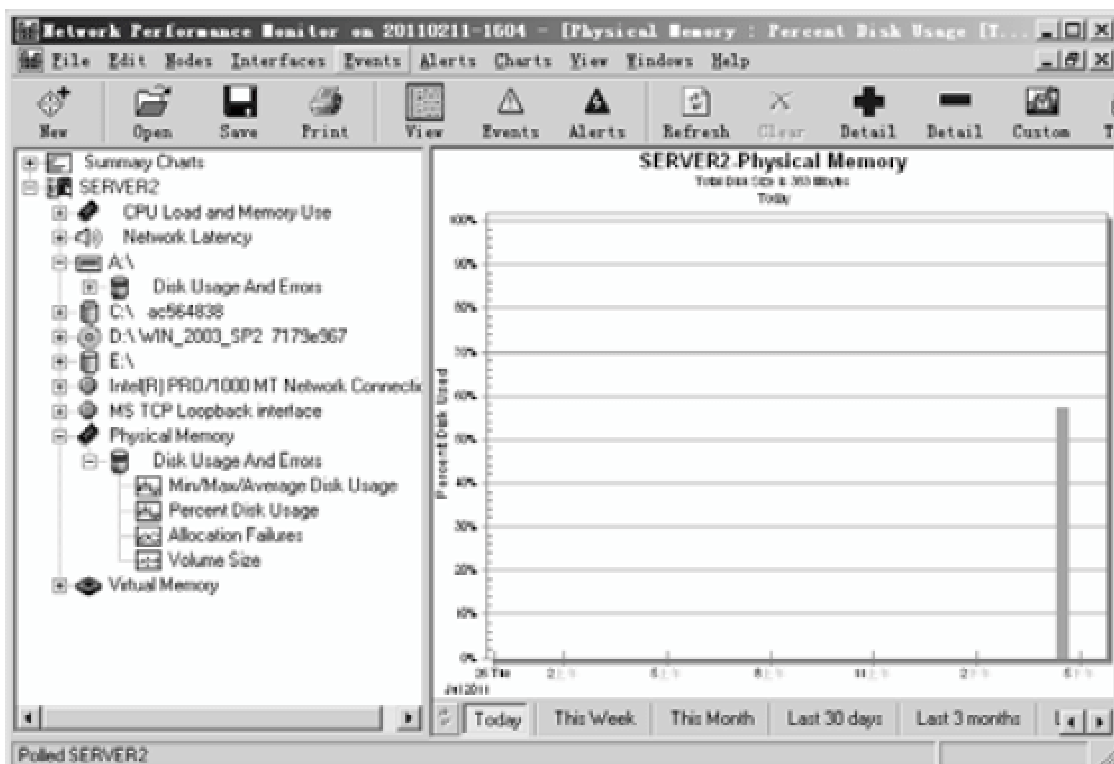


图 16-52 Physical Memory 选项列表

16.3.3 其他网络管理小工具

在 SolarWinds 中小工具非常多，可以通过选择【开始】➢【程序】➢ SolarWinds Engineers ➢ SolarWinds Toolbar 选项（见图 16-53），打开如图 16-54 所示的工具集列表框，总共分为 12 类工具，每一类中都有很多可用的小工具，当然这 12 类工具中也有重复。下面介绍几款比较实用的小工具，具体内容如下。

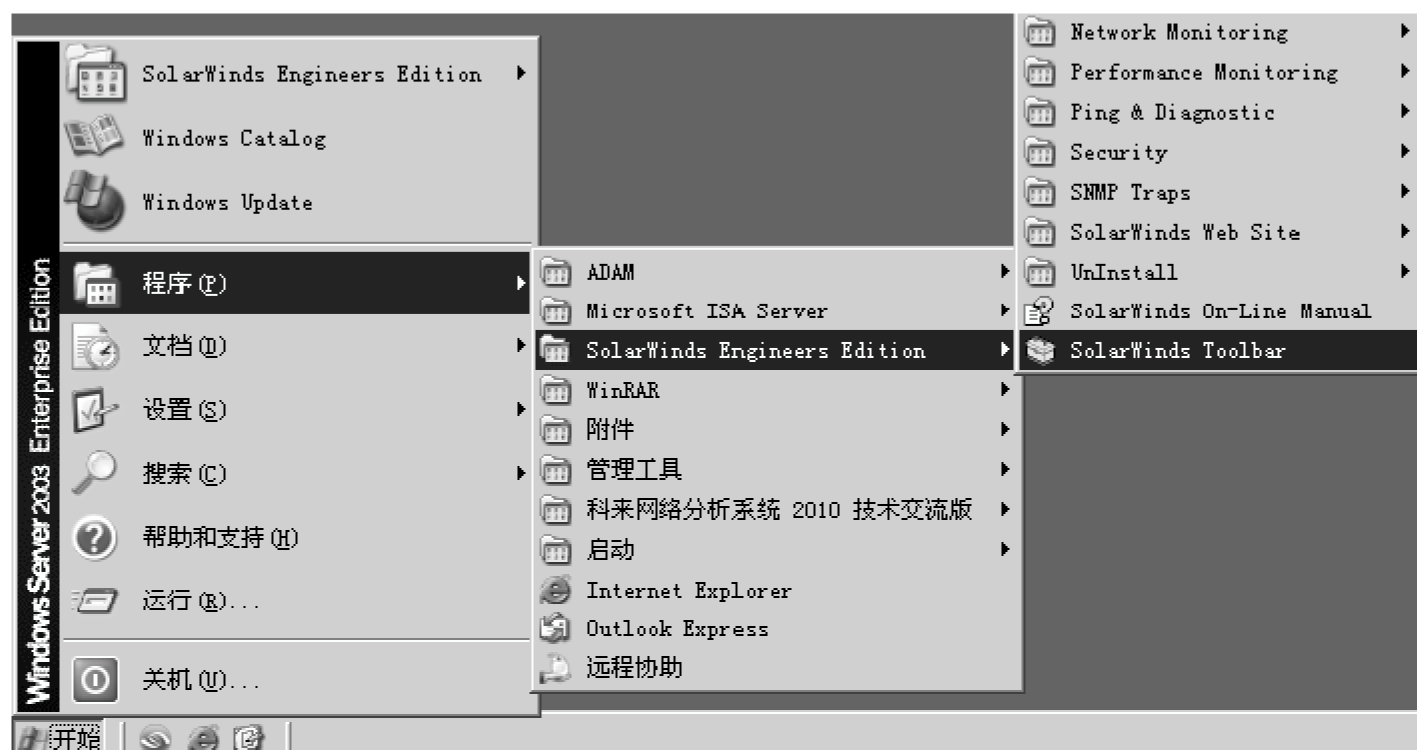




图 16-53 SolarWinds Toolbar 选项

图 16-54 SolarWinds 工具集列表

1. Ping Sweep

Ping Sweep 用于检测某个 IP 范围内的地址是否在使用中，并可反查其主机域名，具体操作方

法如下。

01 单击 SolarWinds 工具集列表中的 Ping Sweep 工具，弹出 Ping Sweep 提示框，单击 Close 按钮，如图 16-55 所示。

02 打开 Ping Sweep 窗口，在 Starting IP Address 和 Ending IP Address 文本框中输入地址范围，在 Scan For 下拉列表中选择扫描要求，本实例选择 Responding IPs（所有相应 IP）选项，单击 Scan 按钮，如图 16-56 所示。

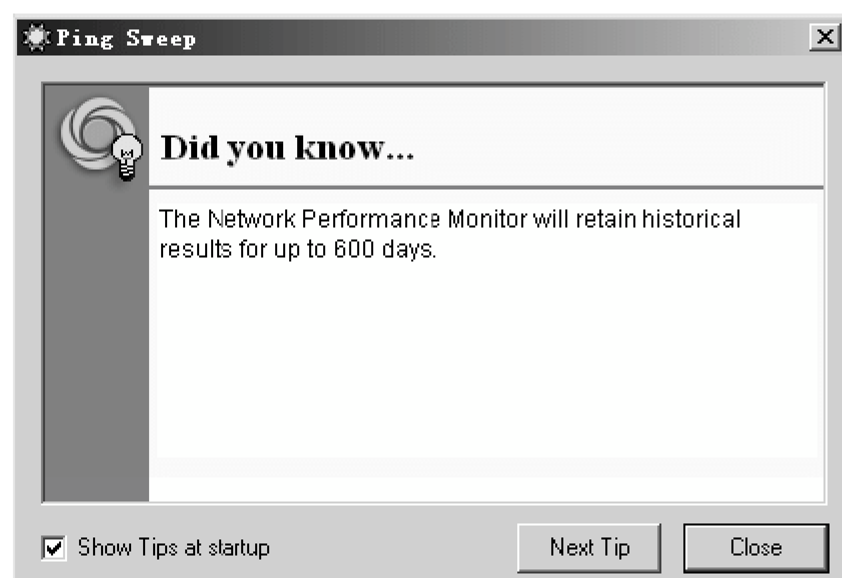


图 16-55　Ping Sweep 提示框

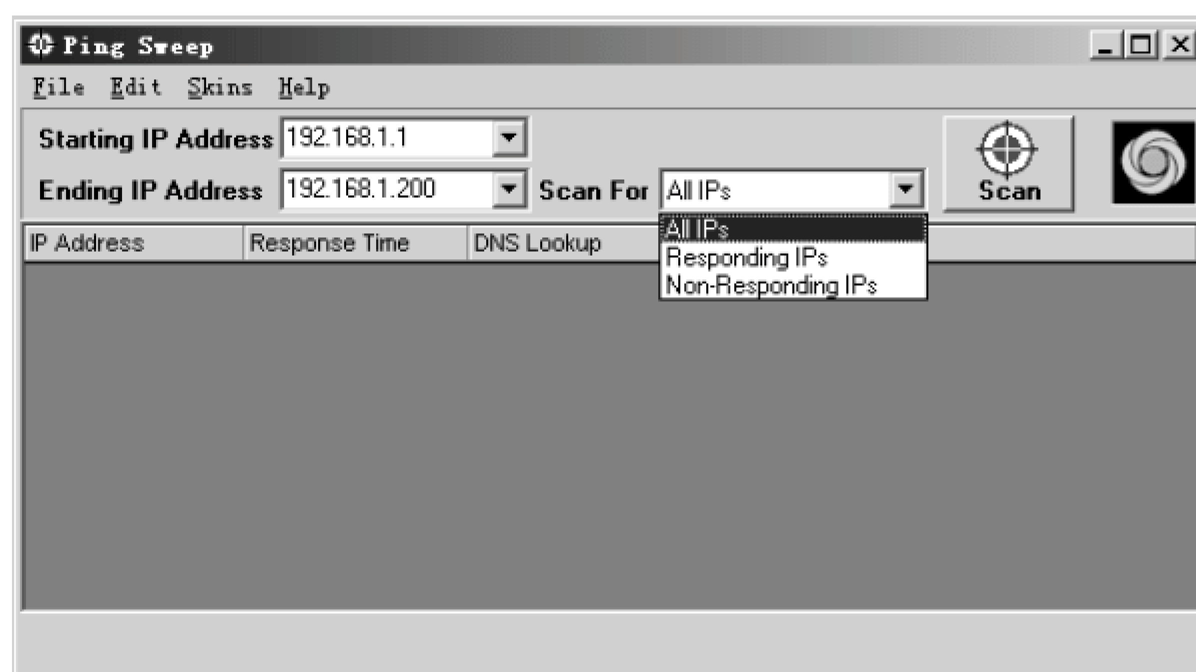


图 16-56　Ping Sweep 窗口

03 如图 16-57 所示，扫描结束，共扫描到 5 台主机，其中两台有 DNS 解析名。

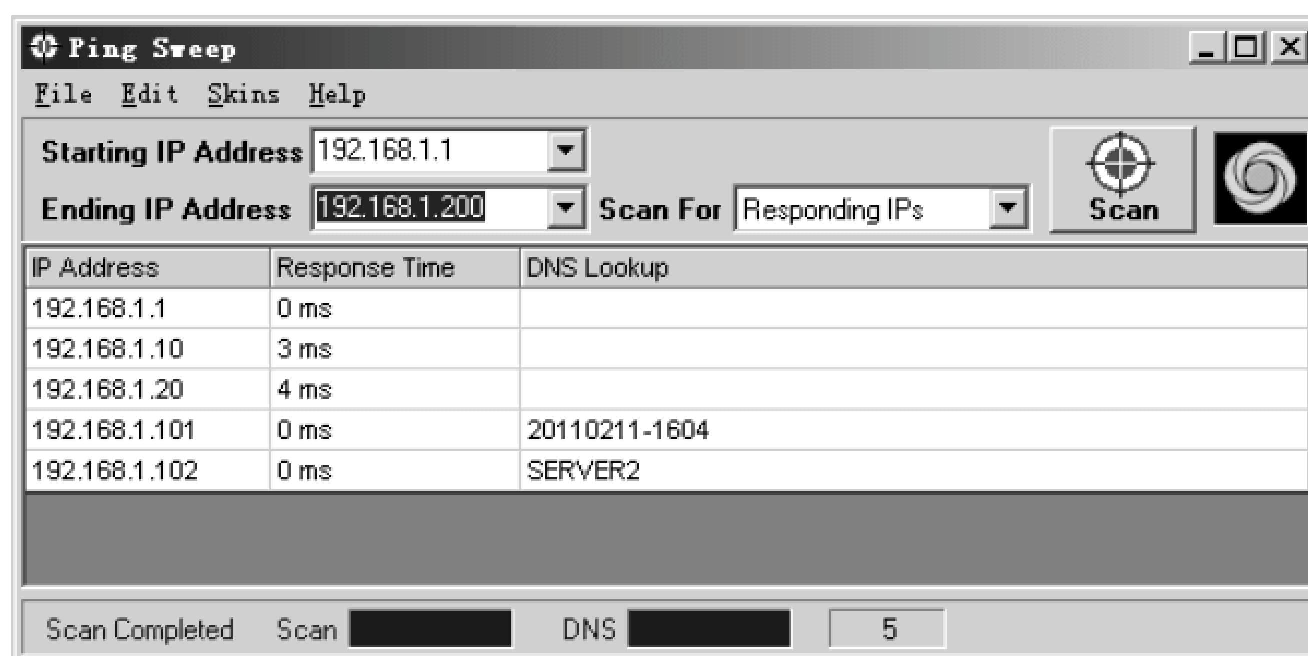


图 16-57　目标网段扫描结束

04 右击需要查询的主机地址，在弹出的快捷菜单中可以选择使用相应工具作进一步的管理操作，如选择【IP Network Browser】命令查看目标主机信息，如图 16-58 所示。

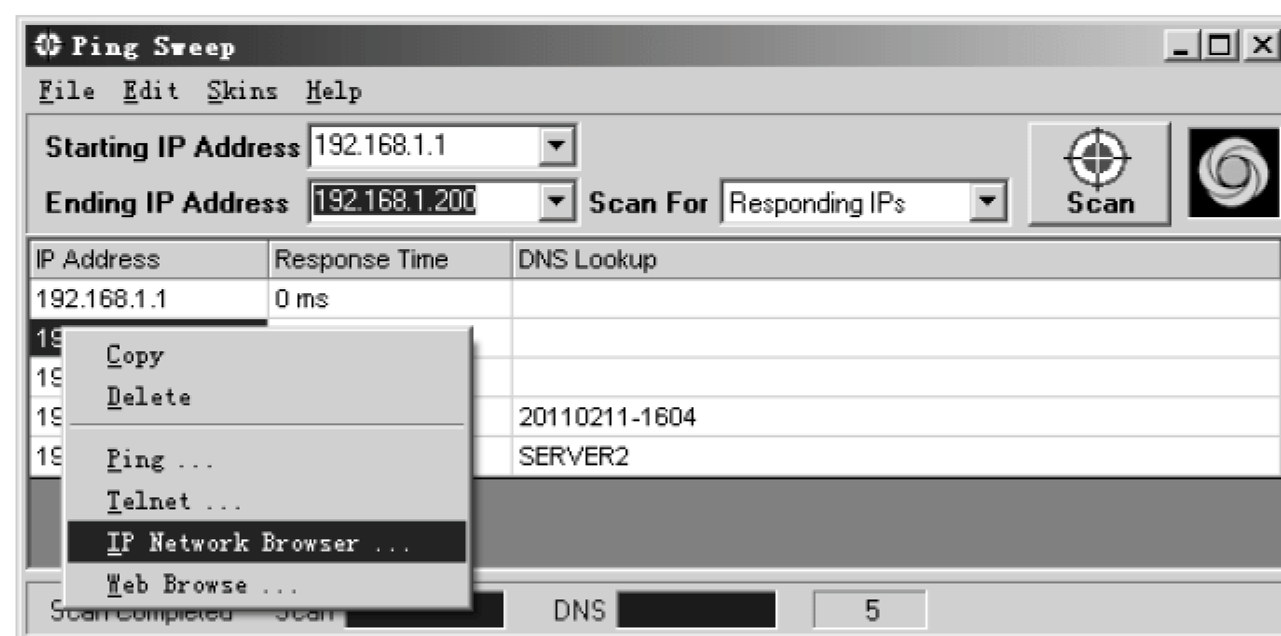


图 16-58　快捷菜单工具

2. Subnet List

Subnet List 工具主要用于查看目标主机所在网段，以及其所在网段的广播地址等信息，具体操作步骤如下。

01 单击 SolarWinds 工具集列表中的 SubnetList 工具，弹出 SubnetList（子网列表）提示框，单击 Close 按钮，如图 16-59 所示。



图 16-59　SubnetList 提示框

02 打开 SubnetList 窗口，在 Hostname or IP Address 文本框中输入目标主机 IP 地址，在 SNMP Community String 文本框中输入 SNMP 的团体名，单击 Retrieve Subnets 按钮，如图 16-60 所示。



图 16-60　SubnetList 窗口

03 显示扫描结果，扫描结果中包括目标主机所在的网段是 192.168.1.0/24 网段，广播地址为 192.168.1.255，如图 16-61 所示。

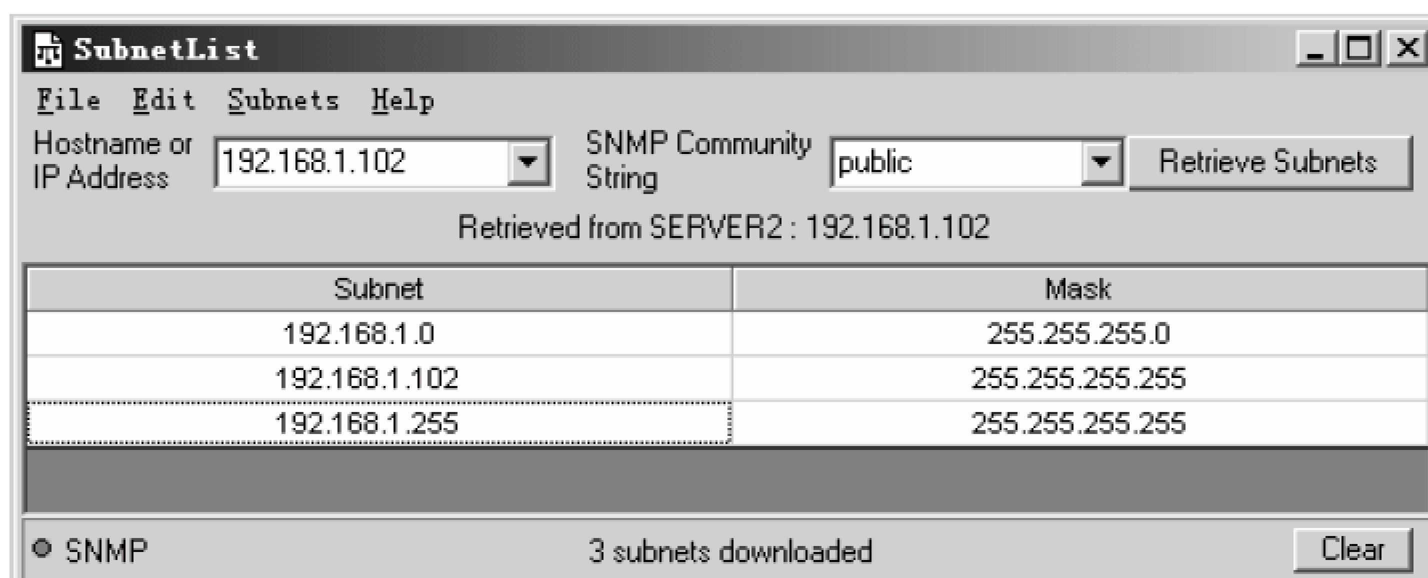


图 16-61　子网列表扫描结果

3. SNMP Sweep

SNMP Sweep 用于检测某个 IP 范围内的地址是否在使用中，以及这些地址对应的主机的系统

信息、主机域名解析等内容，具体操作方法如下。

01 单击 SolarWinds 工具集列表中的 SNMPSweep 工具，弹出 SNMPSweep 提示框，单击 Close 按钮，如图 16-62 所示。

02 打开 SNMPSweep 窗口，在 Starting IP Address 和 Ending IP Address 文本框中分别输入扫描网段的起始地址和结束地址，单击 Scan 按钮，如图 16-63 所示。



图 16-62　SNMPSweep 提示框

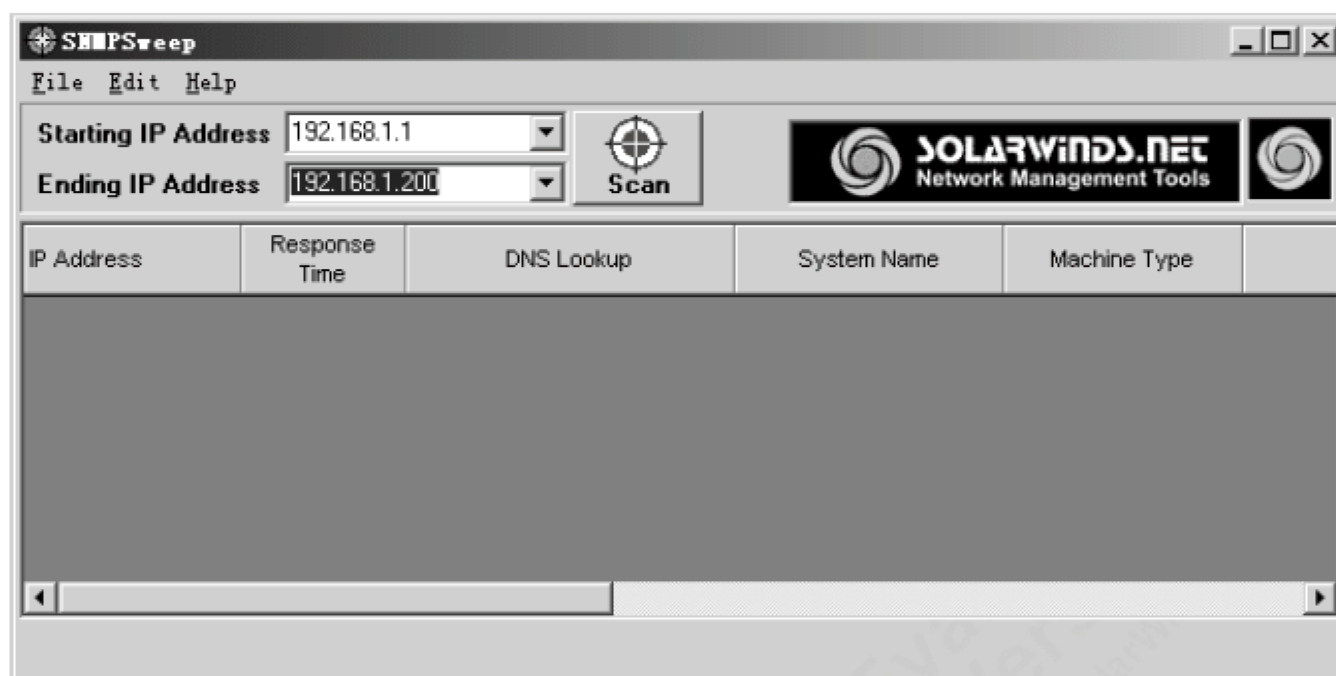


图 16-63　SNMPSweep 窗口

03 扫描结束，显示扫描结果，扫描结果中包括扫描到的主机 IP 地址、请求响应时间、主机解析名、系统类型、最后一次启动时间、团体名称等信息，如图 16-64 所示。

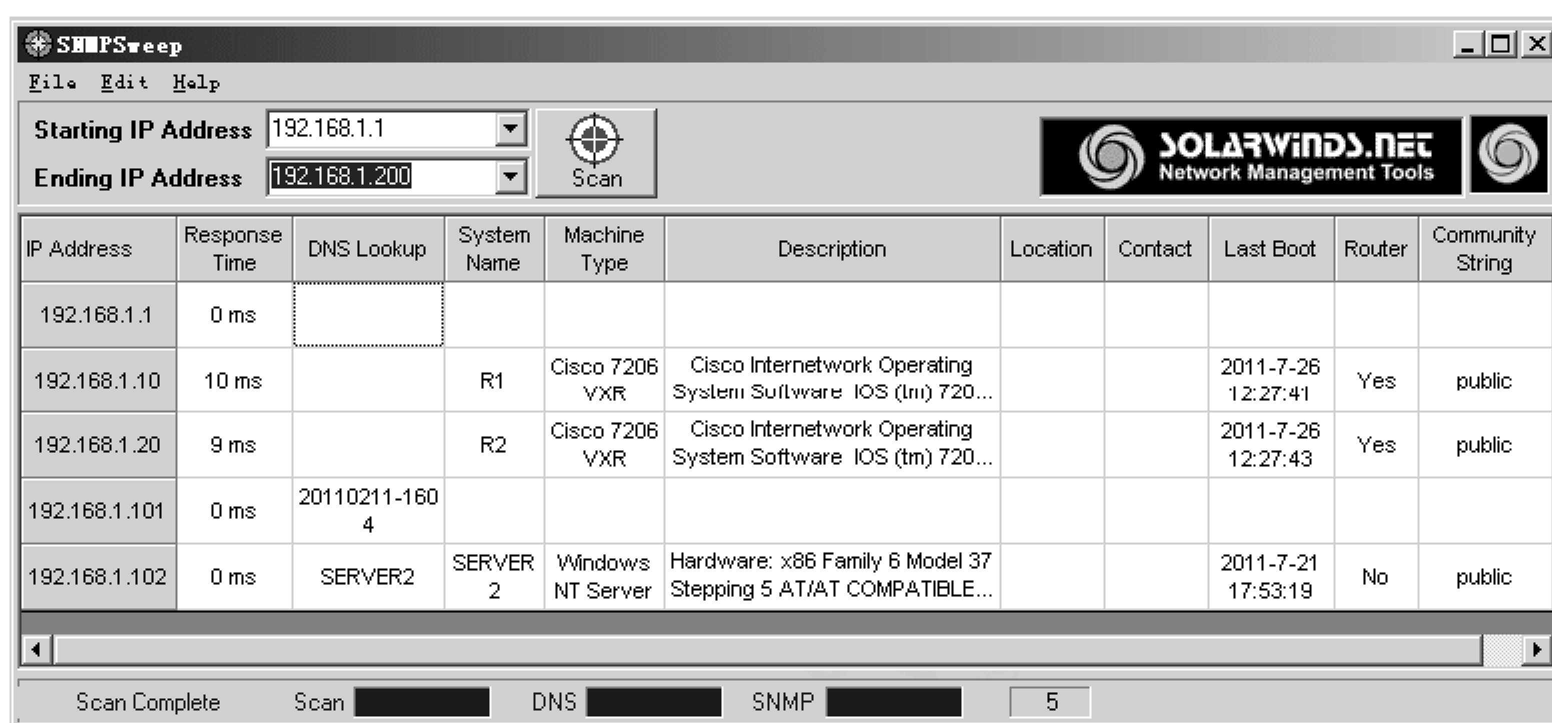


图 16-64　目标网段扫描结果

4. MAC Address Discovery

MAC Address Discovery（MAC 地址发现）工具主要用于查看本地子网中所有已联网主机的 MAC 地址，具体操作步骤如下。

01 单击 SolarWinds 工具集列表中的 MAC Address Discovery 工具，弹出 MAC Address Discovery 提示框，单击 Close 按钮，如图 16-65 所示。

02 打开 MAC Address Discovery 窗口，在 Local Subnet 文本框中输入需要扫描的本地网段，单击 Discover MAC Addresses 按钮，如图 16-66 所示。



图 16-65　MAC Address Discovery 提示框



图 16-66　MAC Address Discovery 窗口

03 扫描结束，显示的扫描结果中包括扫描到的主机 IP、MAC 地址、DNS 解析名等信息，如图 16-67 所示。

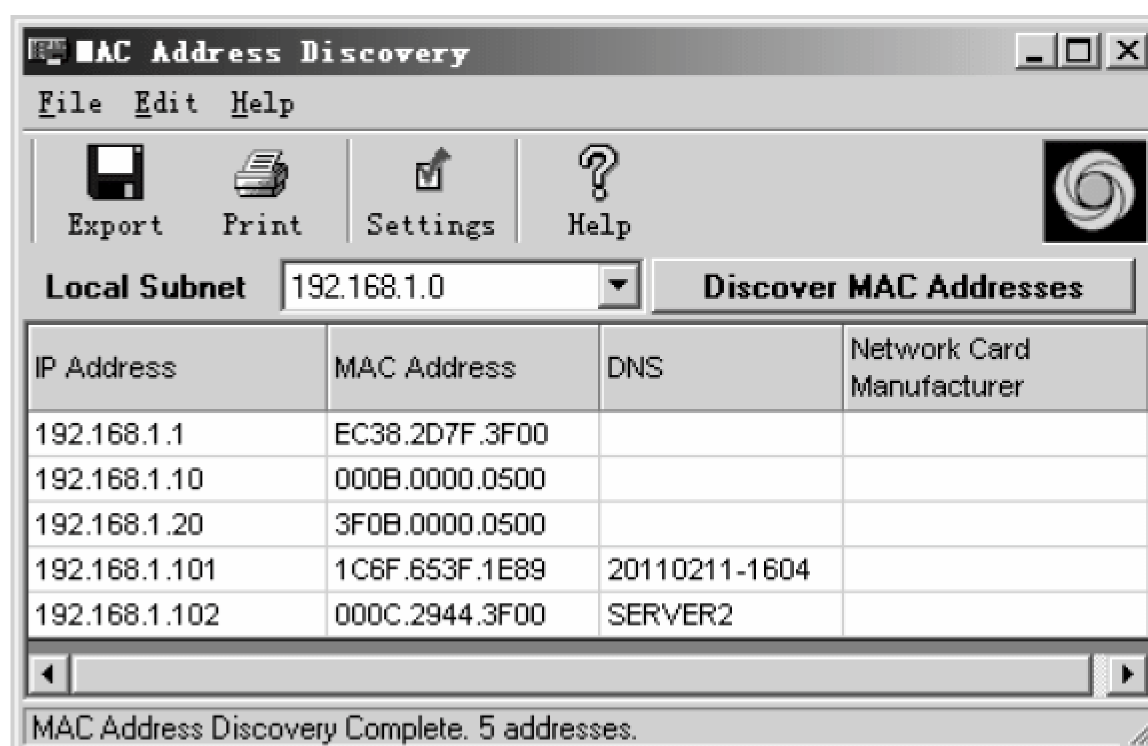


图 16-67　本地子网主机 MAC 地址扫描结果

5. CPU Gauge

CPU Gauge（CPU 负荷监视器）工具主要用于实时监视目标主机 CPU 的使用情况，一般用于监视服务器的 CPU，该程序比较简单直观，具体操作方法如下。

01 单击 SolarWinds 工具集列表中的 CPU Gauge 工具，弹出 SolarWinds CPU Load Monitor（SolarWinds CPU 负荷监视器）提示框，单击 Close 按钮，如图 16-68 所示。



图 16-68　SolarWinds CPU Load Monitor 提示框

02 弹出 CPU Gauge 工具窗口，单击右上方的配置按钮，弹出快捷菜单，选择 Setup Gauge 命令，如图 16-69 所示。

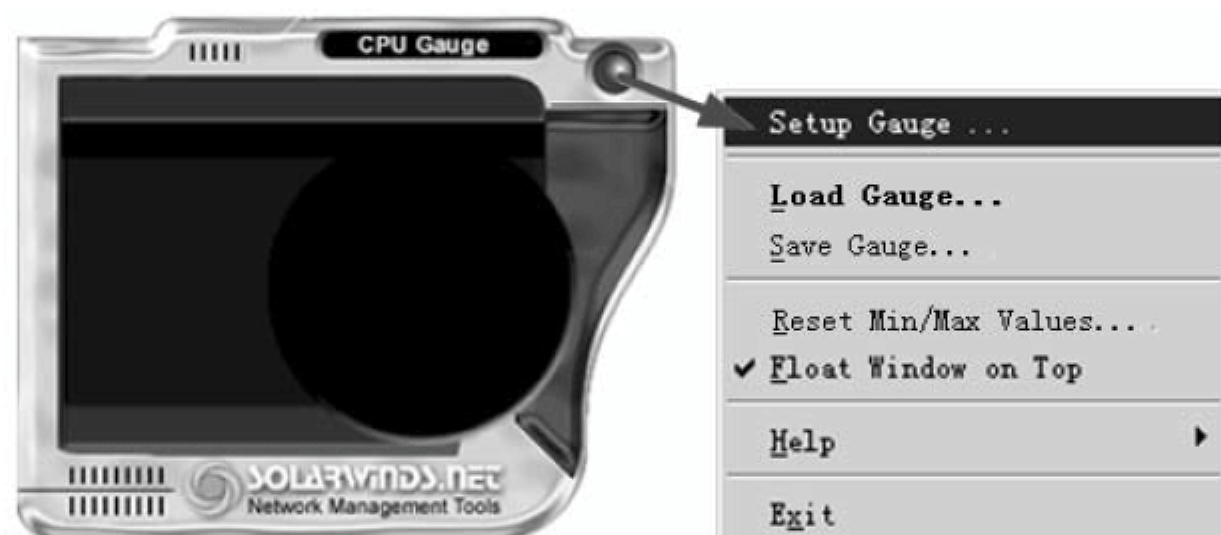


图 16-69 CPU Gauge 工具窗口

03 弹出 Setup CPU Gauge 对话框，在 IP Address or Hostname 文本框中输入目标主机的 IP 地址，在 SNMP Community String 文本框中输入目标主机的 SNMP 共同体名，单击 OK 按钮，如图 16-70 所示。

04 目标主机连接成功，开始监控。显示目标主机名为 “SERVER2” ，Max 表示最大 CPU 使用率，Min 表示最小 CPU 使用率，如图 16-71 所示。

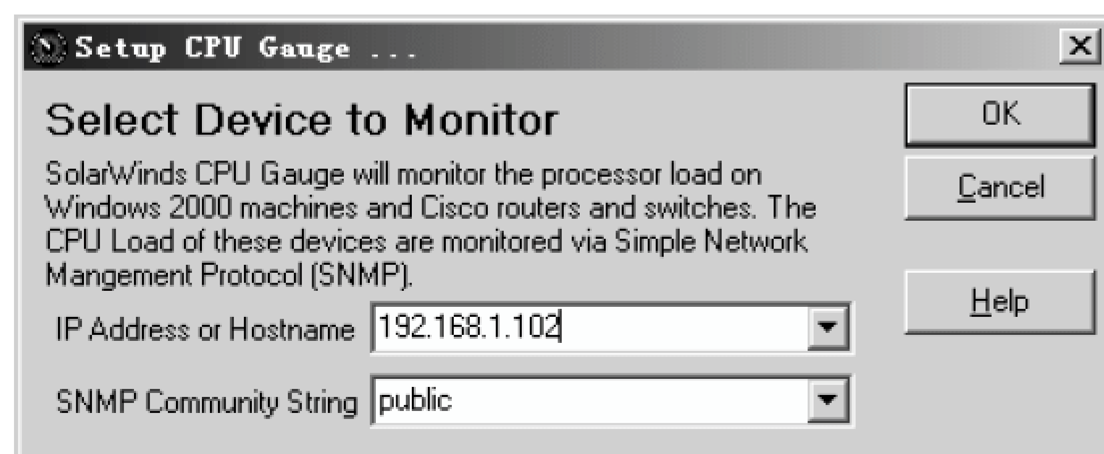


图 16-70 Setup CPU Gauge 对话框

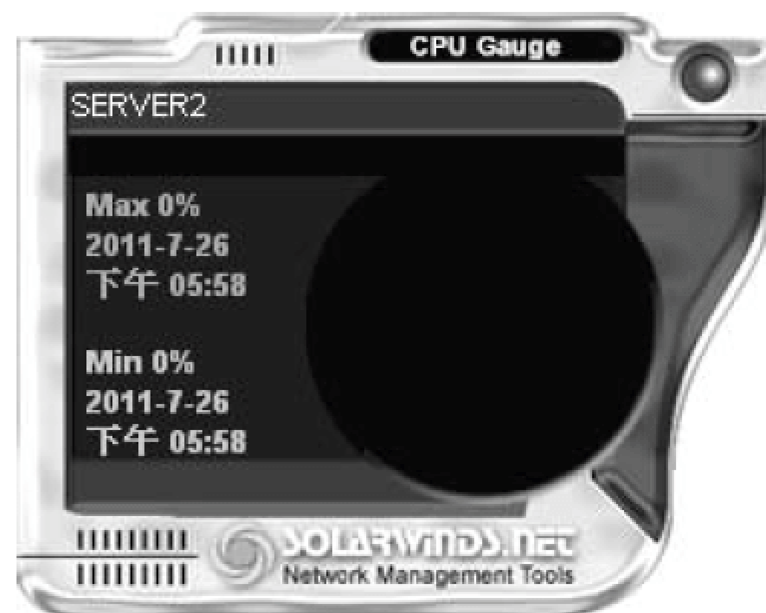


图 16-71 开始监视目标主机 CPU

6. Enhanced Ping

Enhanced Ping（增大的 ping）工具可以实现同时向多个主机发送 ping 请求，并监视响应时间，具体操作步骤如下。

01 单击 SolarWinds 工具集列表中的 Enhanced Ping 工具，弹出 Enhanced Ping 提示框，单击 Close 按钮，如图 16-72 所示。

02 弹出 Enhanced Ping 窗口，单击工具栏 Add/Edit 按钮，如图 16-73 所示。

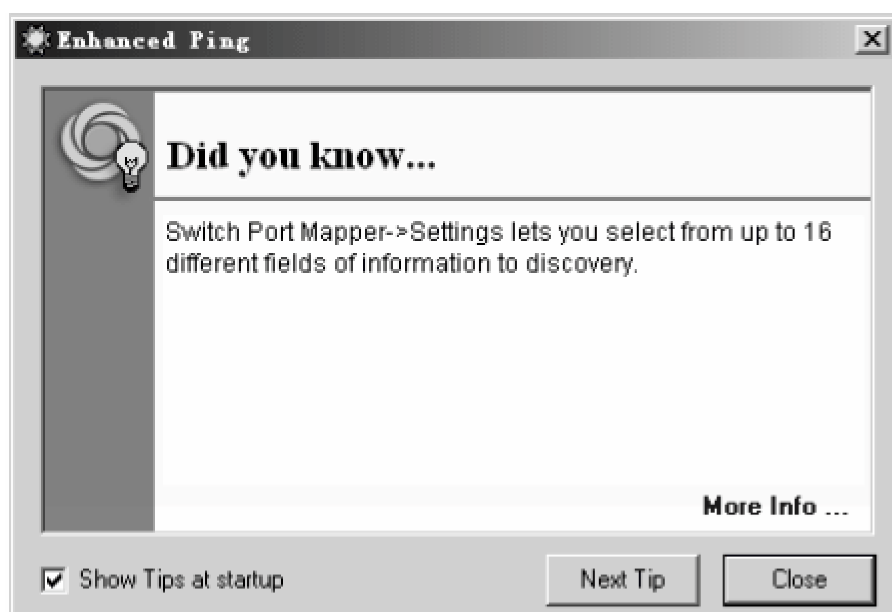


图 16-72　Enhanced Ping 提示框

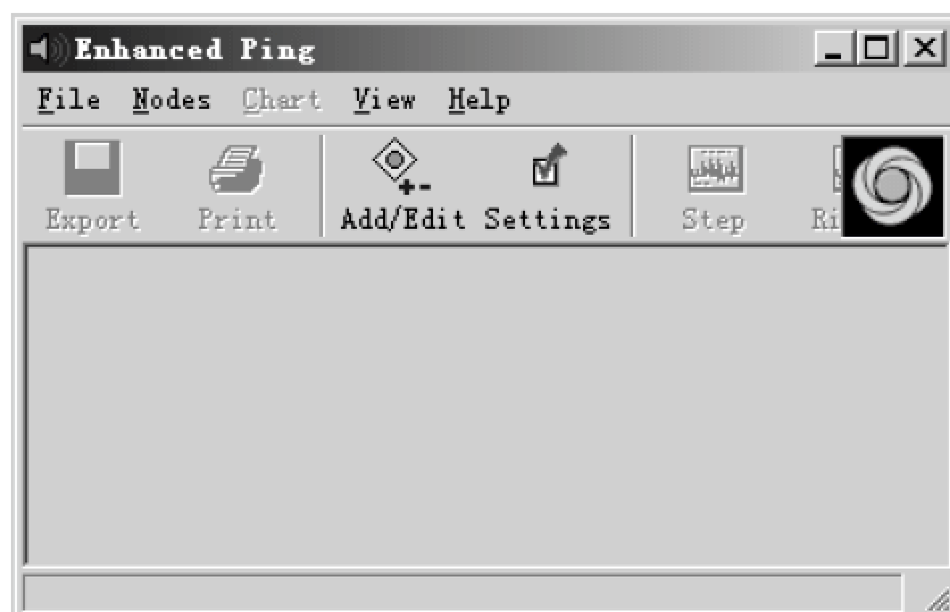


图 16-73　Enhanced Ping 窗口

03 弹出 Add/Delete/Edit Nodes 对话框，在下方文本框中输入要 ping 的目标主机 IP 地址，单击 Add Node 按钮，可同时添加多个，添加后会在上方列表框中显示，添加完成后单击 OK 按钮，如图 16-74 所示。

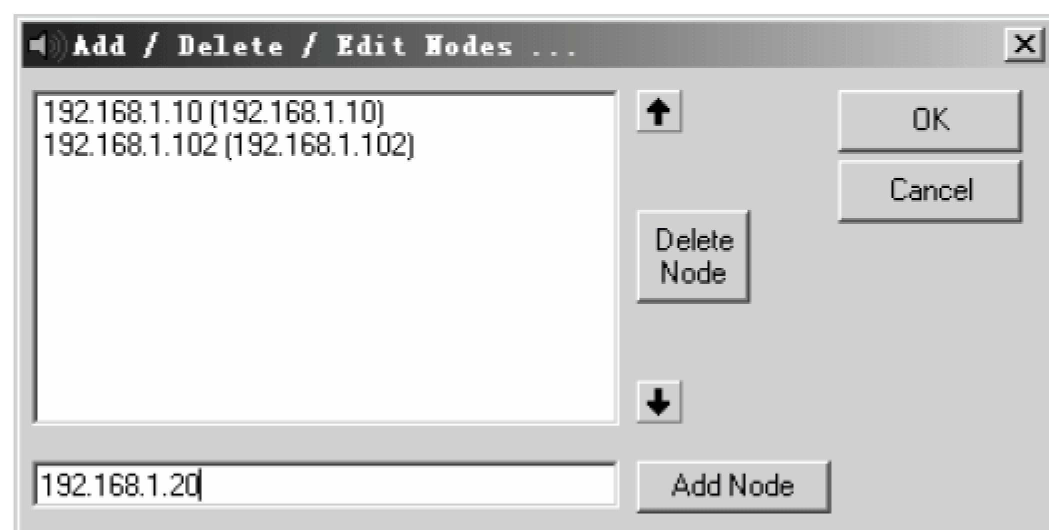


图 16-74　Add/Delete/Edit Nodes 对话框

04 对添加的三个目标主机进行 ping 操作，并以不同颜色的曲线显示其 ping 数据包延迟时间，这些数据可以用来表示到达目标主机的网络性能，如图 16-75 所示。

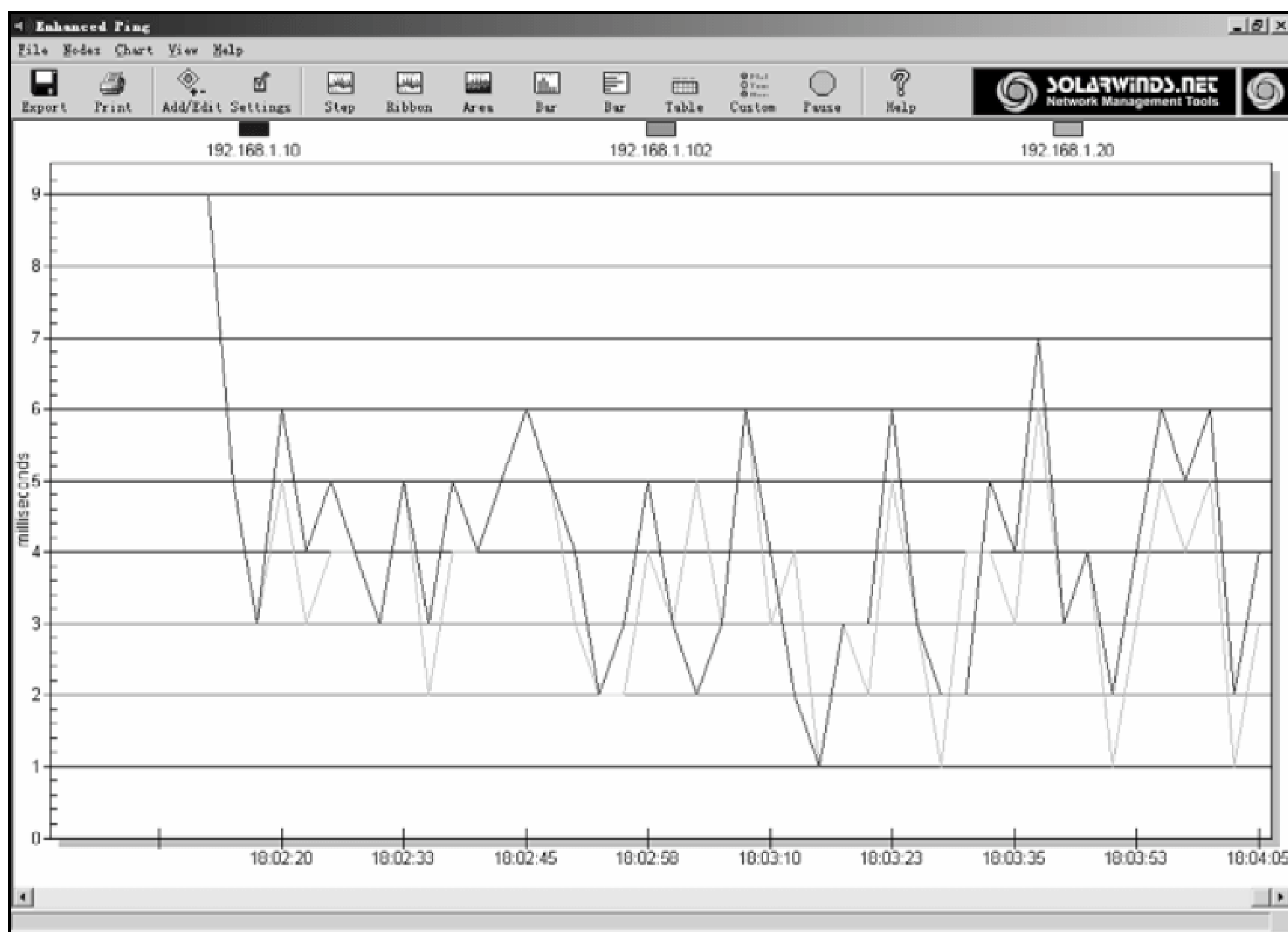


图 16-75　ping 三个目标主机的响应时间

16.4 专家答疑

（1）使用 SolarWinds 工具集是否能够满足所有的网络管理需求？

答：不是，SolarWinds 工具集是一套齐全的管理工具，但是大都是实现单一功能的小工具，很多全面的、系统的管理任务无法完成。所以该工具集只能作为网络管理中的辅助小工具来使用，而且很多系统的企业网络管理程序中包含了 SolarWinds 工具集中的很多功能。

（2）SolarWinds 工具集中的工具这么多，是否都可用？

答：该工具集中的工具大都可以使用，但是也会出现一些程序连接不成功的现象，其主要原因就是 SNMP 协议的配置，如果在使用该工具集时没有配置 SNMP 协议，那么很多工具将不可用。作为网络管理员应该有选择性地使用该工具，而不是为了使用该工具开放配置所有的 SNMP 协议。

第 17 章　网络管理平台的架设与使用

随着各公司企业网络环境的不断完善，网络规模也在逐步扩大，面对越来越多的网络设备，越来越复杂的网络拓扑结构，传统的管理方式已经显得有些笨拙，如何更有效、更直观地实施网络管理，成为不少技术人员关注的话题。

伴随这些问题，先后出现了很多网络管理工具，其中网络管理平台是网络环境管理中最系统、最直观的工具之一。通过网络管理平台，可以直观地查看到当前网络的动态拓扑结构，实时查看所有网络设备的性能状态，以帮助网络管理员实施网络管理。

17.1　网络管理平台介绍

随着网络技术的发展，网络管理工具层出不穷，但是很多工具在查看网络运行状态上比较被动，网络出现故障时不能通过工具及时表现出来，具体的网络故障点也要运用工具去测试。而网络管理平台却可以动态显示全网的链接状态，一旦出现设备故障或链接故障，都会及时的通过网络管理平台显现出来，大大提高了故障的发现和解决效率。因此，搭建可靠的网络管理平台成为了企业网络管理过程中必不可少的内容。

17.1.1　什么是网络管理平台

网络管理平台也可称为网络运维管理系统。对于运营商的网络环境管理，一般都称为网络运维管理，所以大多数厂商都会运用网络运维管理系统这个名字。

网络管理平台不单单是一个网络管理软件的安装。首先，要使用 SNMP 等网络管理协议搭建一套可管理的网络环境。其次，要在网络中指定的网络管理设备上安装网络管理平台软件。满足以上两点，才算是一套网络管理平台系统。

通过网络管理协议，网络管理平台可以获取所有网络设备、服务器、主机的运行状态及其性能参数。但是网络管理平台的产品比较繁杂，功能也有所差异。

具体来说，网络管理平台的主要功能有以下几个方面。

1. 真实动态的网络拓扑管理

利用网络管理平台，可以自动生成全网的物理拓扑结构，动态实时反映网络布线信息、设备运行状态及链路的流量变化情况等，帮助网络管理员一目了然地掌控整个网络的实时运行状态。

图 17-1 所示为使用 Spiceworks 软件获取的网络拓扑图。

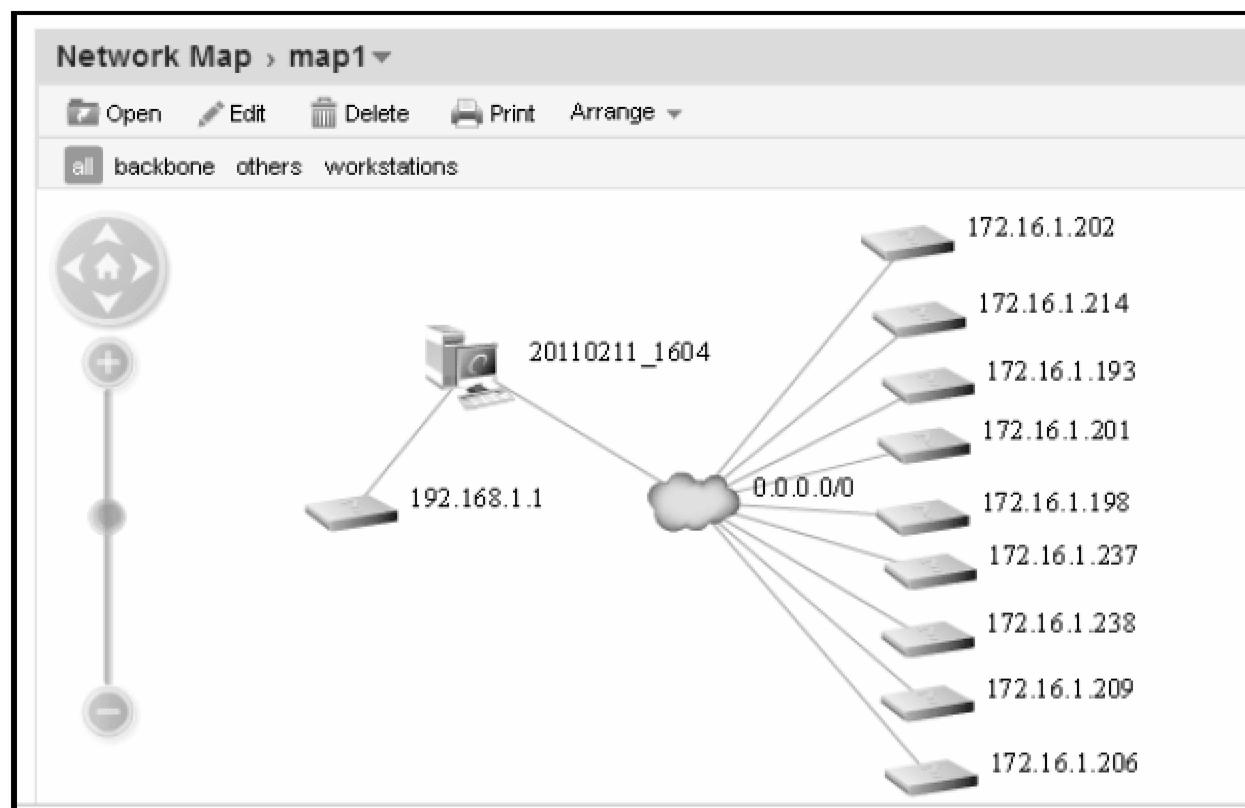


图 17-1　Spiceworks 软件获取的网络拓扑图

2. 层次分明的统一管理

当网络的管理区域相当庞大时，通过网络管理平台可以实现分层、跨地域的管理。上层网络管理员可以概括地看到各大区域的链接状况，也可以细化地看某一区域内的拓扑结构。

3. 多厂商设备的全面管理

设备管理是网络平台管理的核心。大多数网络管理平台都只是 SNMP 网络管理协议，只要设备运行了 SNMP 管理协议，就可以被网络管理平台监控，和设备的厂商没有直接关系。

4. 全面完善的告警系统

解决网络故障的效率，在网络管理过程中至关重要。当故障发生后再去修复，必然会造成损失。如果在网络运行刚出现异常时就能被发现，故障就会在造成损失前被解决。因此很多网络管理平台都会设置告警系统，对于网络设备异常、网络链接的流量异常、性能异常等均可设置告警。

图 17-2 所示为 Spiceworks 软件的告警配置页面。

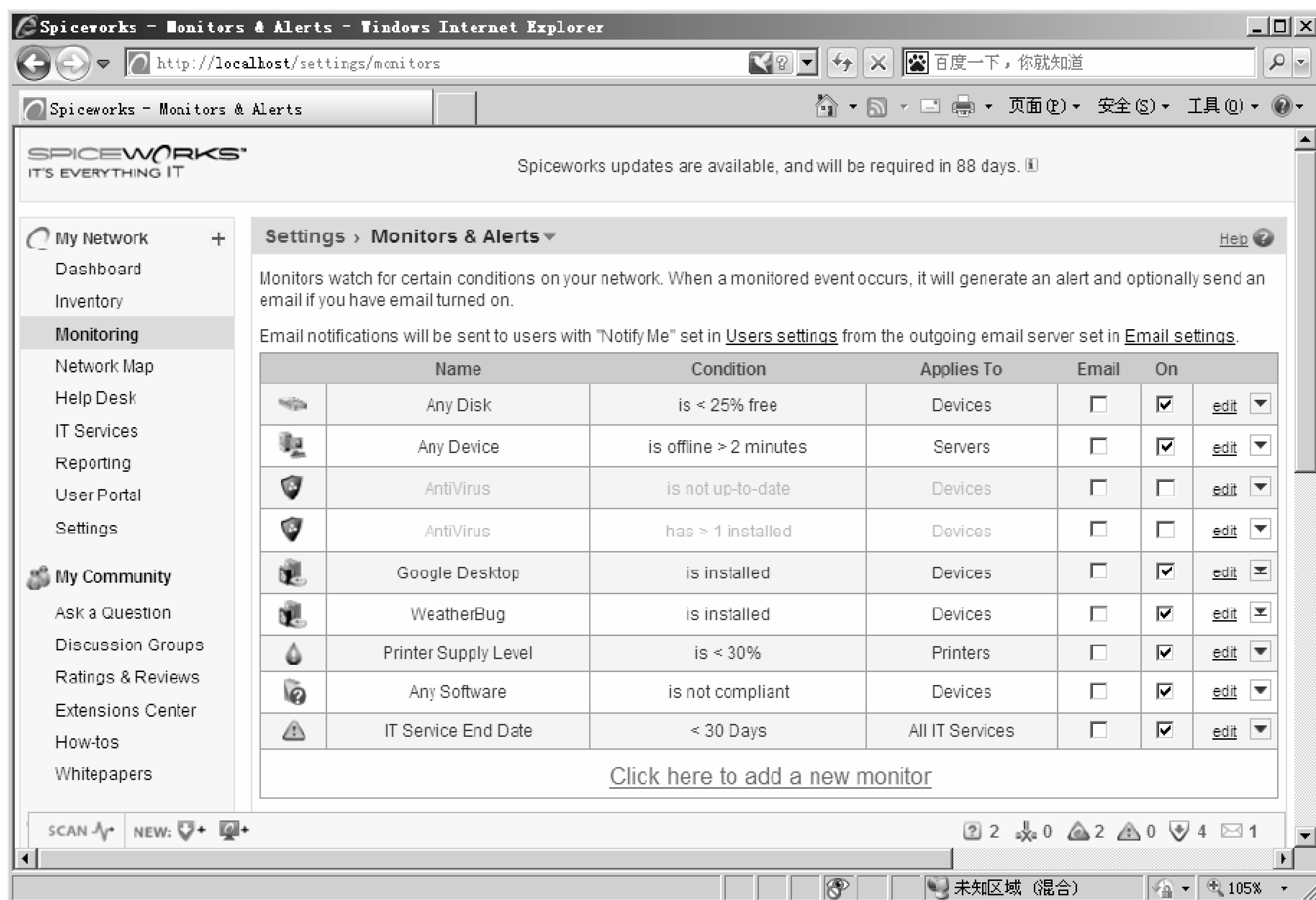


图 17-2　Spiceworks 软件的告警配置页面

5. 全网地址定位的安全管理

网络管理平台可以实现全网 IP 定位、MAC 定位，结合网络安全技术进行安全隐患的排查、捕捉地址盗用及非法设备移动等。

6. 系统的报表查询功能

通过对网络的管理、监控，网络管理平台可以产生各类报表，包括各类性能指标的统计、均量、趋势等。利用这些报表信息，可以有效地分析网络性能状态。

图 17-3 所示为 WhatsUp Gold 软件的事件查看报表。

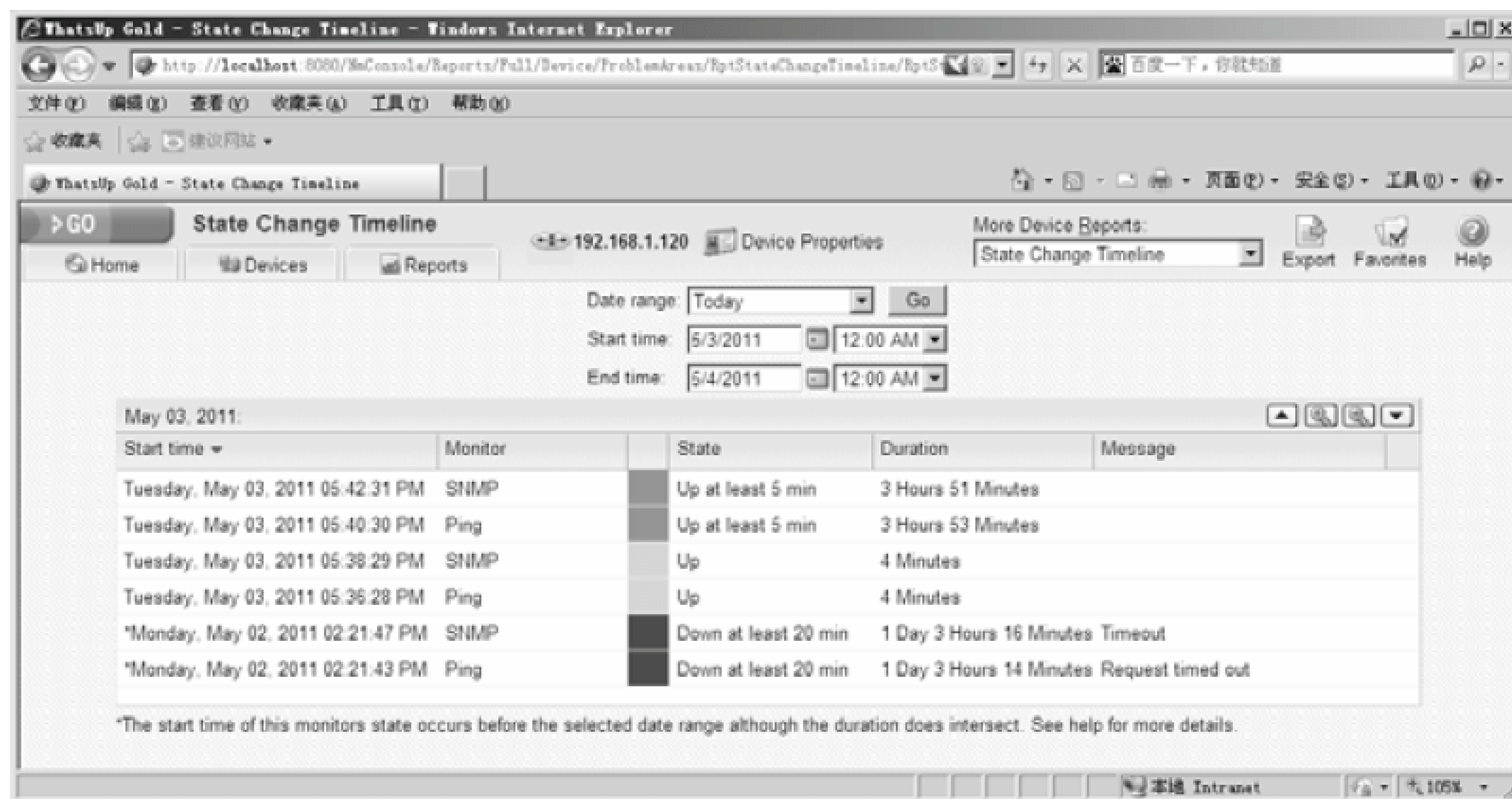


图 17-3　WhatsUp Gold 软件的事件查看报表

7. 异常数据流分析

部分网络管理平台还支持网络流量的抓捕、分析功能，通过数据流量分析，可以发现黑客扫描、病毒扩散、网络攻击，大流量下载等网络问题，并快速地找到问题源。

17.1.2　主流网络管理平台产品

市场上的网络管理平台产品非常多，常见的主流网络产品有以下几个。

1. Spiceworks

Spiceworks 是一款针对中小型企业的网络设备管理和监控软件。它由广告商提供支持，是一款免费软件。根据 Spiceworks 公司的介绍，这款软件适合雇员人数在 250 人以下的中小型企业，其产品功能和特点都是针对这一市场而定制的。

图 17-4 所示为 Spiceworks 网络管理平台的主页面。

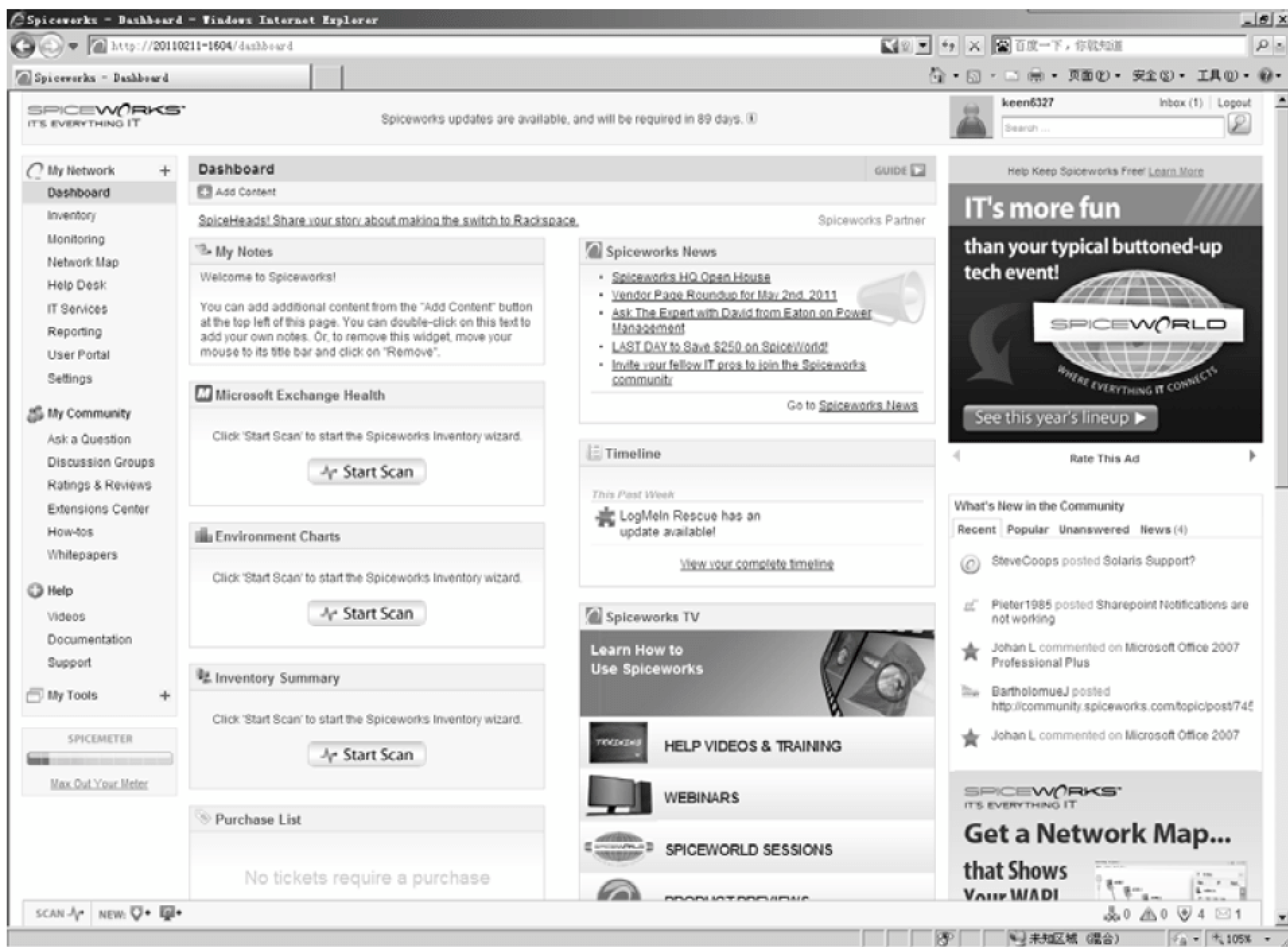


图 17-4　Spiceworks 网络管理平台的主页面

2. WhatsUp Gold

WhatsUp Gold 提供完整、易用的监控机制，全方位监控应用服务与网络设备，协助 IT 管理人员能将网管信息转变成可阅读的商业信息。WhatsUp Gold 能主动监控所有关键网络设备与应用服务，因而减少影响业务运作的停机问题以避免严重损失。WhatsUp Gold 具有操作容易、快速布署、扩充性强、高投资报酬率等优势而独树一帜。

图 17-5 所示为 WhatsUp Gold 网络管理平台查看网络设备的 Web 页面。

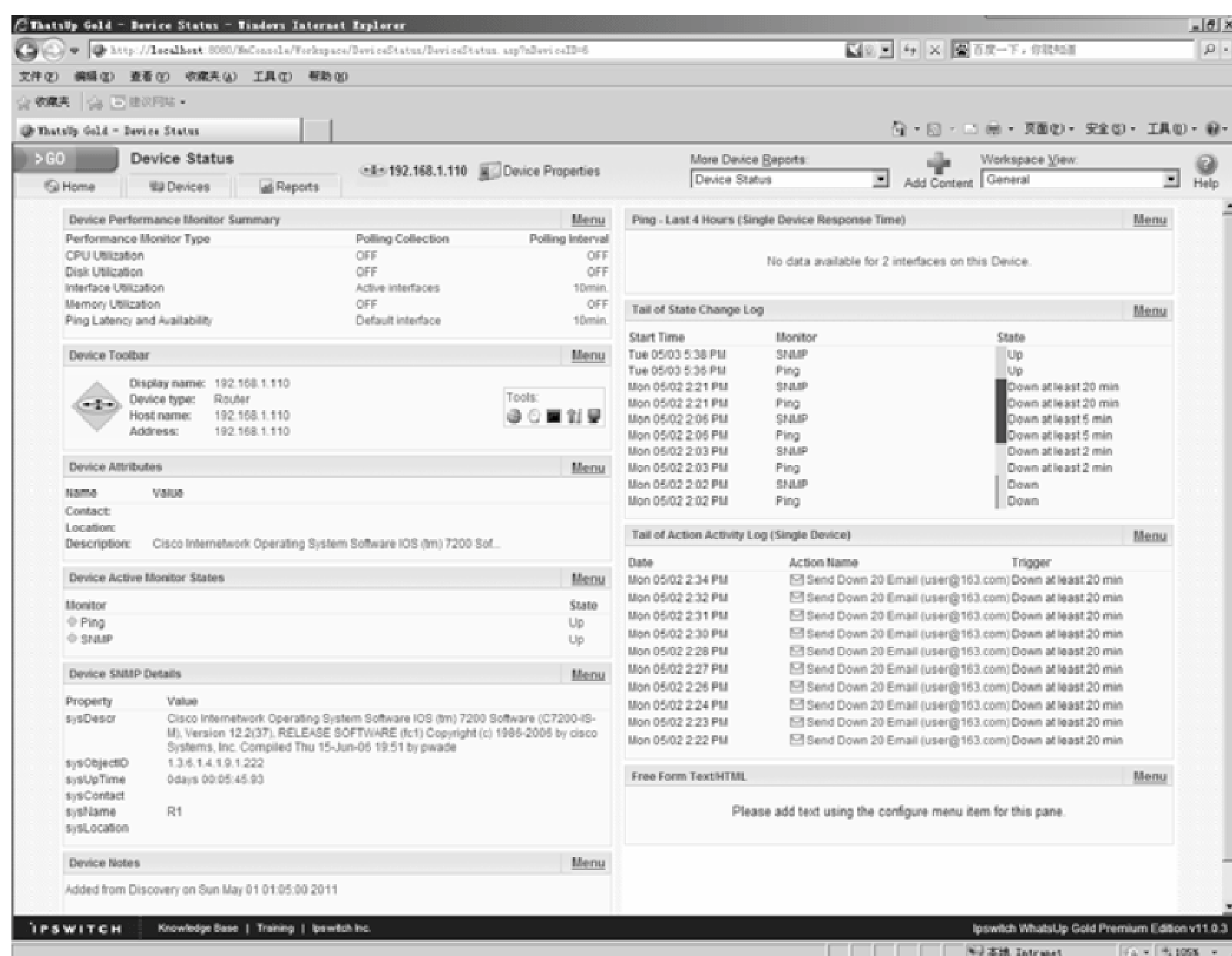


图 17-5　WhatsUp Gold 网络管理平台查看网络设备的 Web 页面

3. HP OpenView

HP OpenView 产品是惠普公司出品的电子业务管理工具程序，被称为“全球 20 大软件公司必备产品”，面向 HP 9000 和 HP e3000 系列服务器的用户群。客户可以利用 OpenView 来管理服务器的应用程序、硬件设备、网络配置和状态，系统性能、业务以及程序维护，还能进行存储管理。HP OpenView 是强大的网络和系统管理工具，是第一个跨平台的网络管理系统。图 17-6 所示为 HP OpenView 程序的主界面。

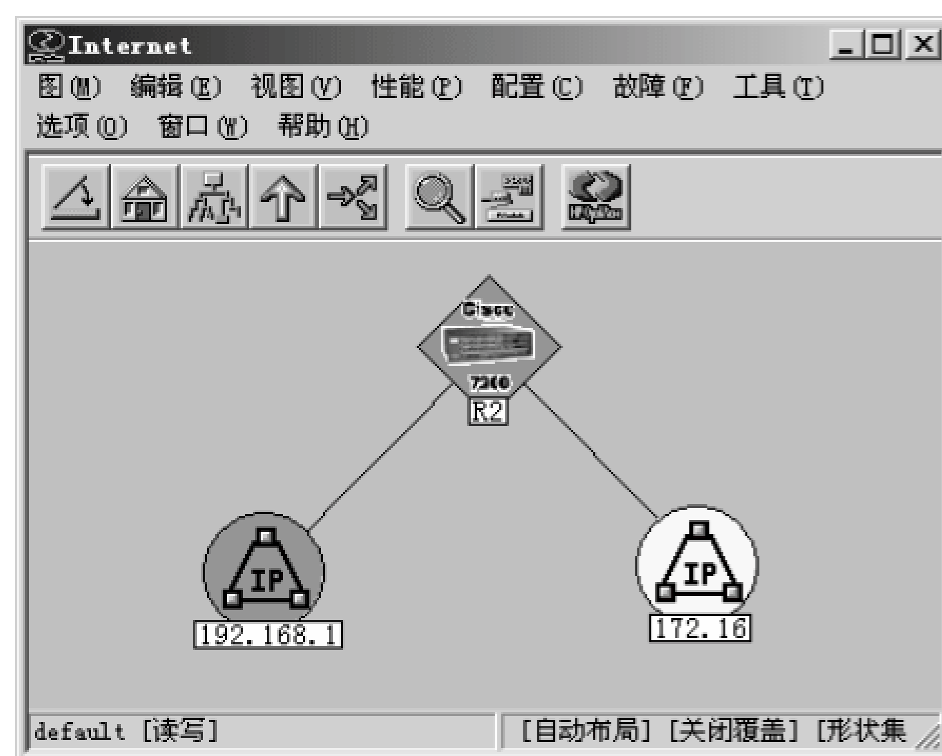


图 17-6　HP OpenView 程序的主界面

4. IBM Tivoli NetView 网络管理系统

IBM Tivoli 是 IBM IT 服务管理的核心部分。Tivoli 是一个跨越主机系统、客户机/服务器系统、工作组应用、企业网络、Internet 服务器的端到端的解决方案。Tivoli 软件为客户提供了一个无缝集

成、灵活的随需应变基础架构管理解决方案，采用强健的安全机制将雇员、业务伙伴和客户连接起来。Tivoli 解决方案主要包括系统管理解决方案，存储管理解决方案和安全管理解决方案。

基于 IBM Tivoli NetView 所提供的网络管理平台，不但能够为用户提供强大的管理能力，而且与 Tivoli 的整体管理框架紧密集成，能够方便地进一步发展到全面的系统管理。

IBM Tivoli 与 Cisco 一直保持着良好的合作关系，NetView 能够与 Ciscoworks2000 紧密集成，实现从 NetView 中调用 CiscoView 和 Campus Manager 等 Ciscoworks 应用，在 NetView 中显示 Cisco 的图标等。

图 17-7 所示为 IBM Tivoli NetView 程序的界面。

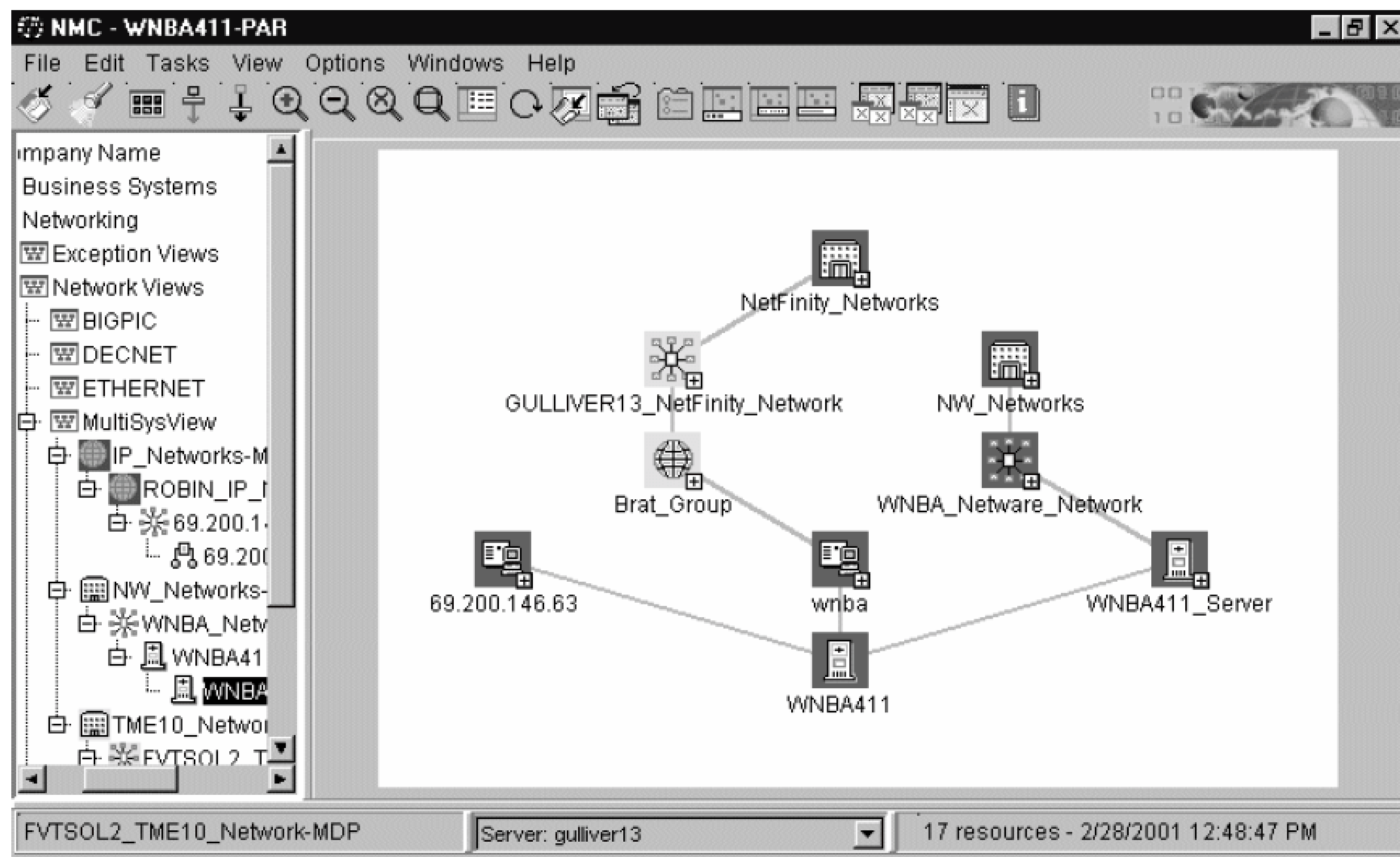


图 17-7　IBM Tivoli NetView 程序的主界面

17.2　项目实战 1：搭建 Spiceworks 网络管理平台

搭建网络管理平台，首先需在公司内部所有网络设备上开启 SNMP 管理协议，然后在指定的网络管理设备上安装网络管理平台软件。下面主要介绍 Spiceworks 网络管理平台的搭建及应用方法。

17.2.1　网络管理环境搭建

在安装 Spiceworks 网络管理平台之前，首先要做好基础网络管理环境的搭建。环境搭建的内容主要有以下几方面。

（1）保证目前的网络状态是全通的。

（2）在所有的被管理设备上开启 SNMP 网络管理协议，并设置团体名为 public。

（3）网络管理设备的机器性能要相对稳定，一般要选择 Windows Server 2003/2008 服务器。

（4）网络管理操作界面以网页形式实现，IE 浏览器要支持 JavaScript、CSS 动态网页的浏览。

17.2.2 架设网络管理平台

网络管理环境搭建完成后，下面就可以架设网络管理平台。在 Windows Server 2003 服务器中架设 Spiceworks 网络管理平台的具体方法如下。

1. 安装 Spiceworks

安装 Spiceworks 的具体步骤如下。

01 运行安装程序进入安装界面。在【spiceworks will run on port number】（spicewords 将要使用的默认端口）文本框中输入连接管理网页所使用的端口，默认值为 80，如图 17-8 所示，单击 Next 按钮。

02 在弹出的对话框中选中 I accept these terms of use and privacy policy 复选框，接受许可协议，如图 17-9 所示，单击 Next 按钮。

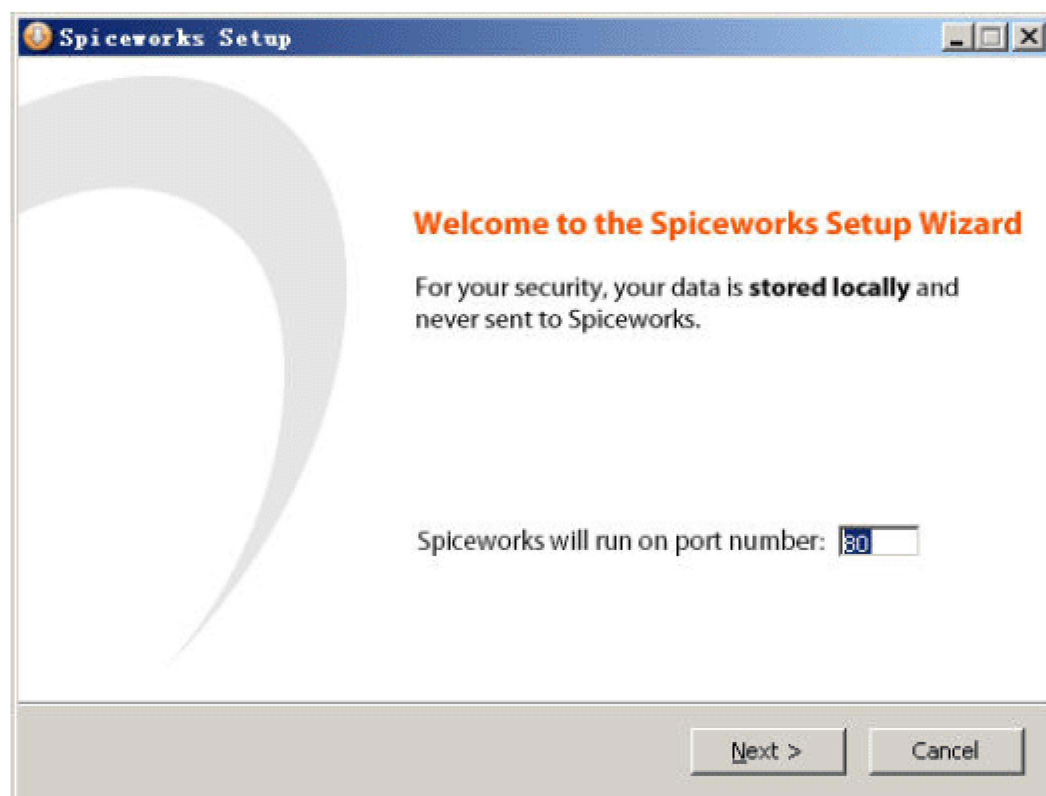


图 17-8 Spicewords Setup 安装向导

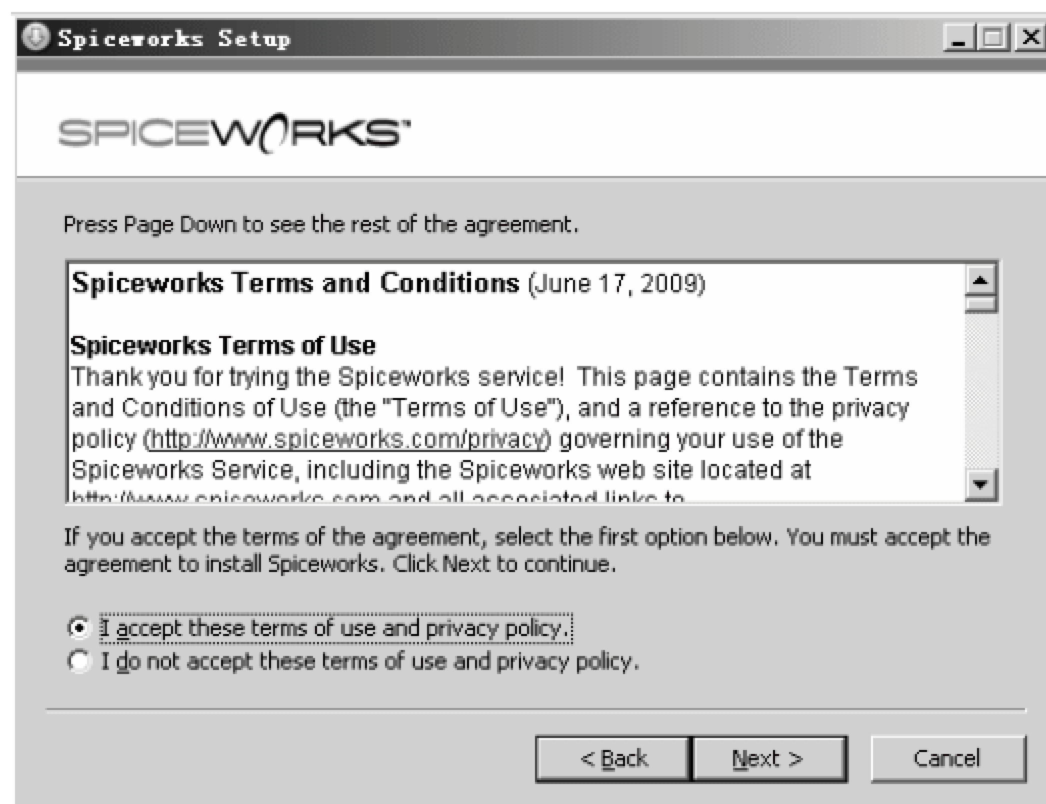


图 17-9 接受许可协议对话框

03 在弹出的对话框中单击 Browse 按钮，可以选择安装路径。本实例选择默认的安装路径，如图 17-10 所示，单击 Install 按钮。

04 系统开始自动安装 Spiceworks，并显示安装的进度，如图 17-11 所示。

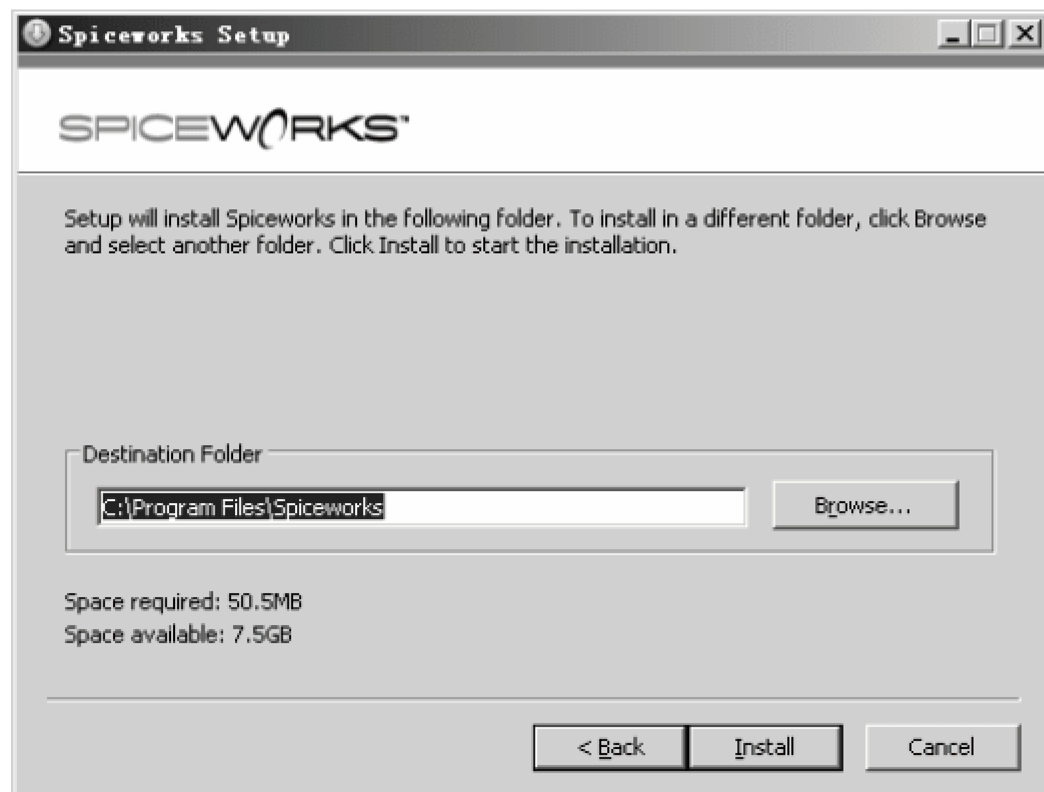


图 17-10 选择安装目录

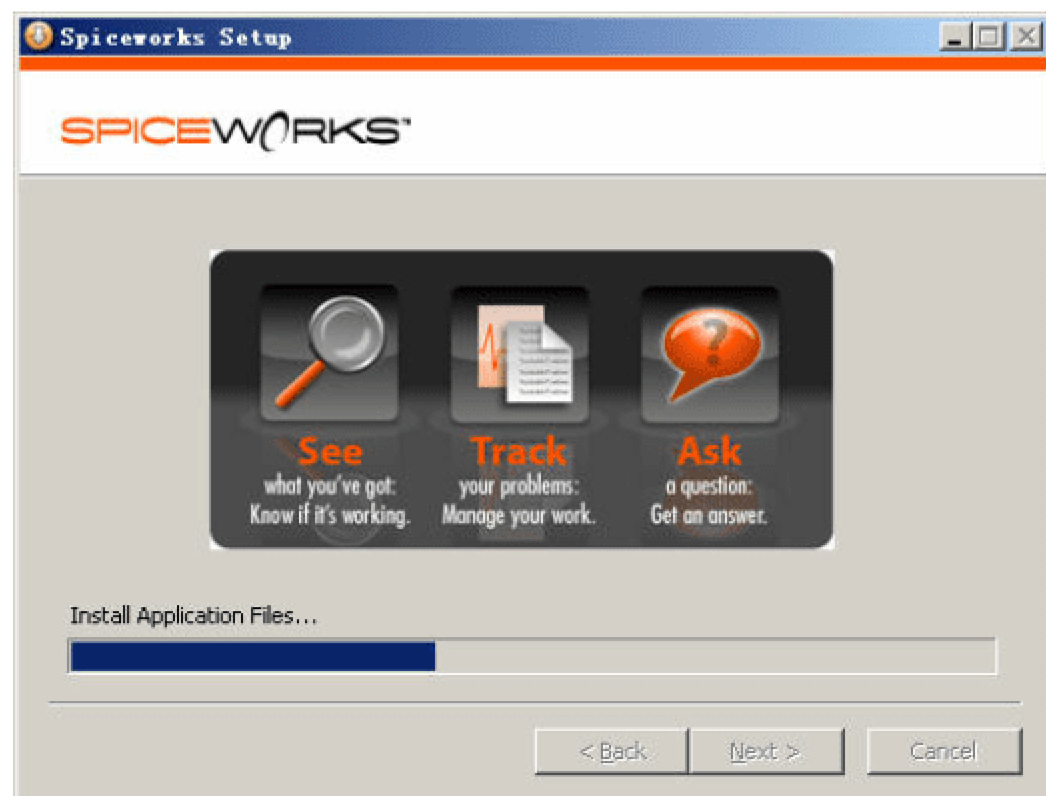


图 17-11 Spiceworks 安装进度

05 安装完成后，在弹出的对话框中选中 Install Desktop Shortcut（创建桌面快捷方式）和 Run Spiceworks Now（马上运行 Spiceworks）复选框，如图 17-12 所示，单击 Finish 按钮。

06 系统自动启动 Spiceworks 网络管理平台，并显示加载的进度，如图 17-13 所示。

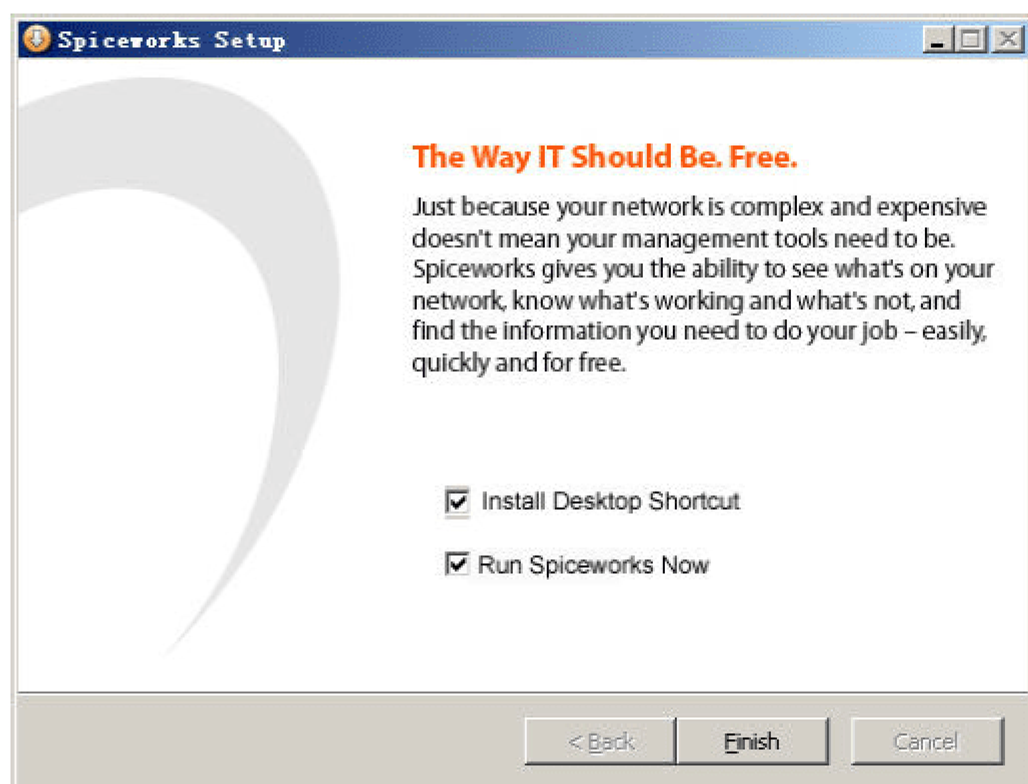


图 17-12　完成安装向导



图 17-13　启动 Spiceworks 网络管理平台

07 加载完成后，登录到 Spiceworks 网络管理平台后自动弹出用户信息录入网页，在页面中分别输入相应的信息，单击 Next 按钮，如图 17-14 所示，Spiceworks 网络管理平台的安装已经完成。

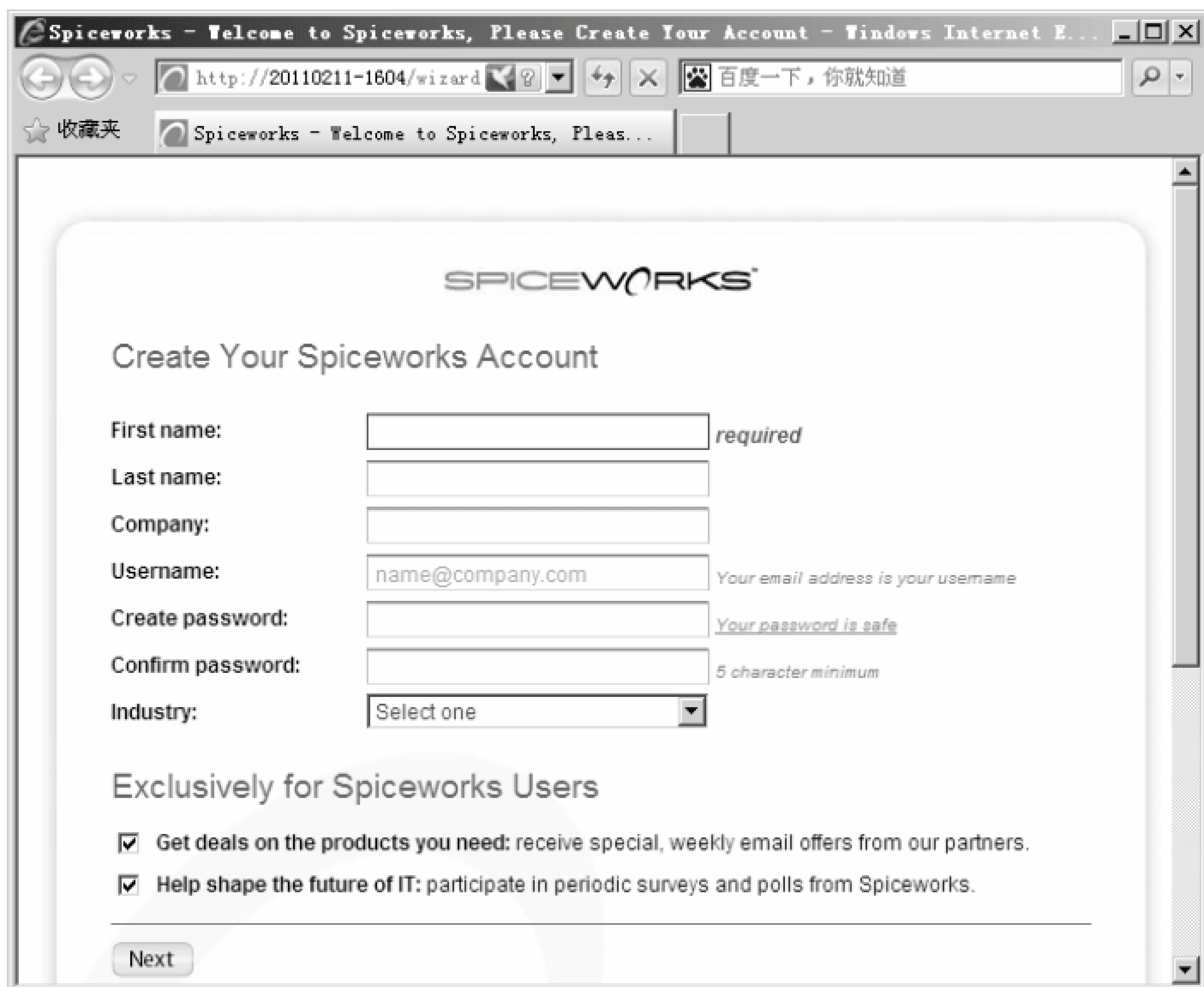


图 17-14　Spiceworks 网络管理平台用户信息录入

页面中各个参数的含义如下。

- First name（名字）：录入用户名字。
- Last name（姓氏）：录入用户姓氏。
- Company（公司）：录入所在公司。
- Username(用户名)：设定登录 Spiceworks 网络管理平台的用户名，格式为邮箱地址，此地

址尽量为可用地址。

- Create password（输入密码）：设定登录密码。
- Confirm password（重新输入密码）：确认密码。
- Industry（行业）：选择应用行业。

2. 网络扫描

刚安装好的 Spiceworks 网络管理平台没有任何网络环境信息，需要进行网络扫描获得网络环境信息。第一次使用 Spiceworks 网络管理平台进行网络扫描的具体操作步骤如下。

01 用户信息设置完成后，进入 Spiceworks 环境页面，选择 Start with Inventory（以清单形式开启）选项，如图 17-15 所示。

02 第一次进入管理页面，没有设备信息清单，会弹出 What would you like to Inventory（如何获得清单）页面，单击 Scan my entire network（扫描全部网络）超级链接，如图 17-16 所示。

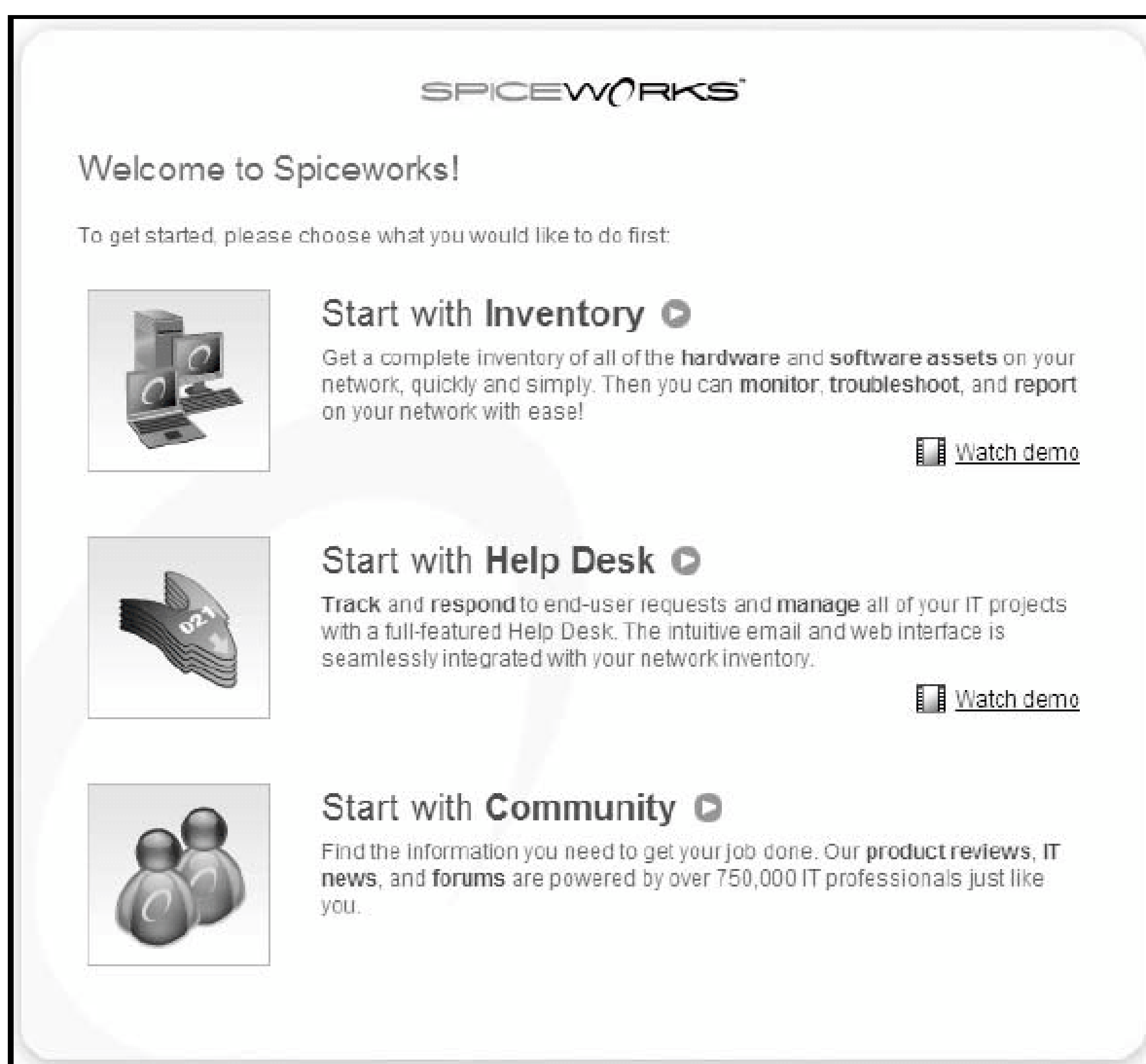


图 17-15　选择打开程序页面方式



图 17-16　设置获得设备清单方式

03 弹出 Scan Settings（扫描设置）页面。根据网络的实际情况选择不同的系统。如果本地主机都是使用 Windows 系统，设置如图 17-17 所示，单击 Next 按钮。

04 如果本地主机有 UNIX/Linux 等系统，设置如图 17-18 所示，并在 Username 和 Password 文本框中输入使用 SSH 连接该系统使用的用户名及密码，单击 Next 按钮。

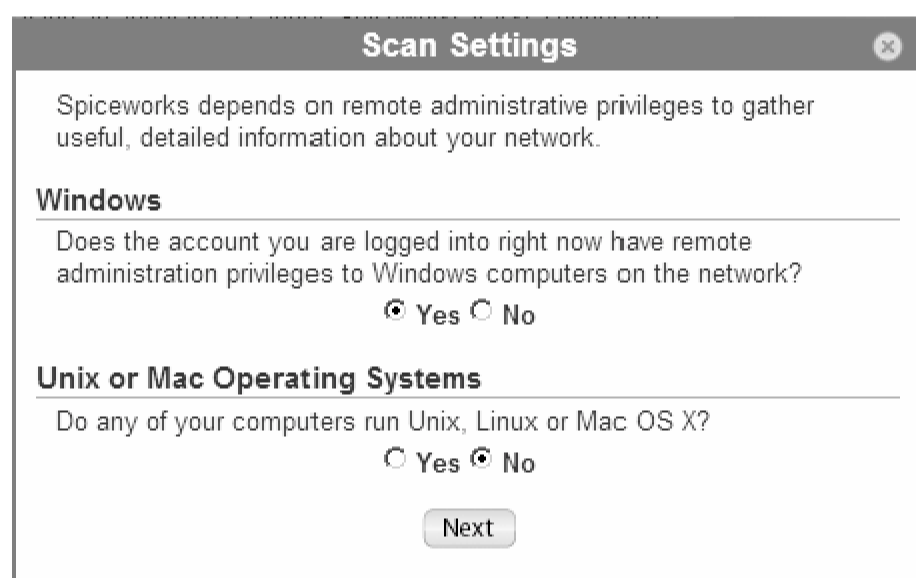


图 17-17　Scan Settings 页面

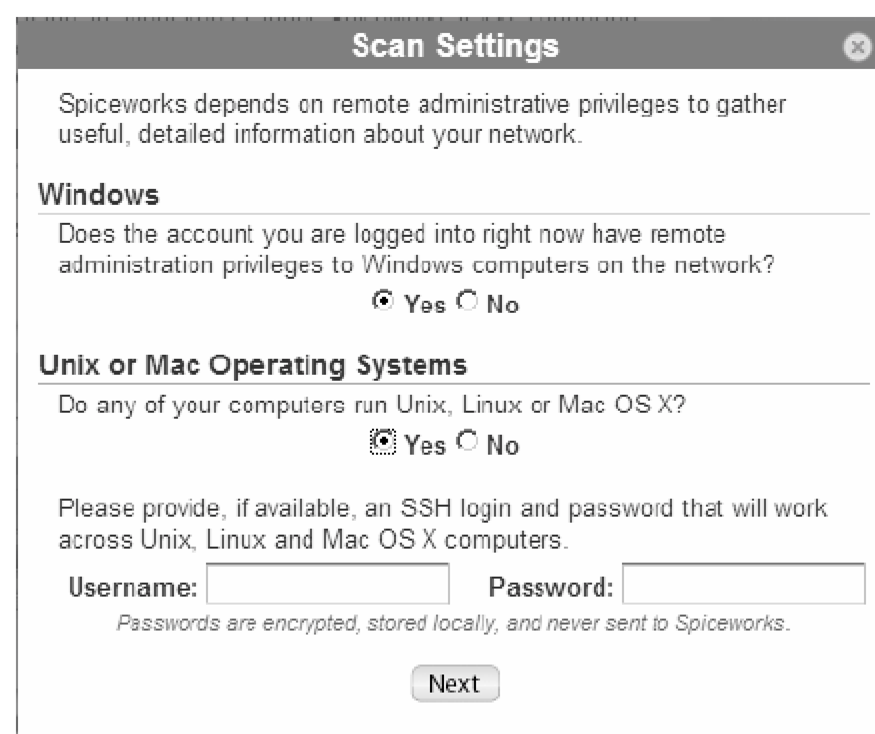


图 17-18　设置获得设备清单方式

05 弹出 Getting ready to inventory your network（准备库存网络）页面，默认对该服务器所在网段“192.168.1.1-254”范围内的所有设备进行扫描，单击 Start 按钮，如图 17-19 所示。

06 弹出 Spiceworks Updates（Spiceworks 更新提示）页面，单击 OK 按钮，如图 17-20 所示。

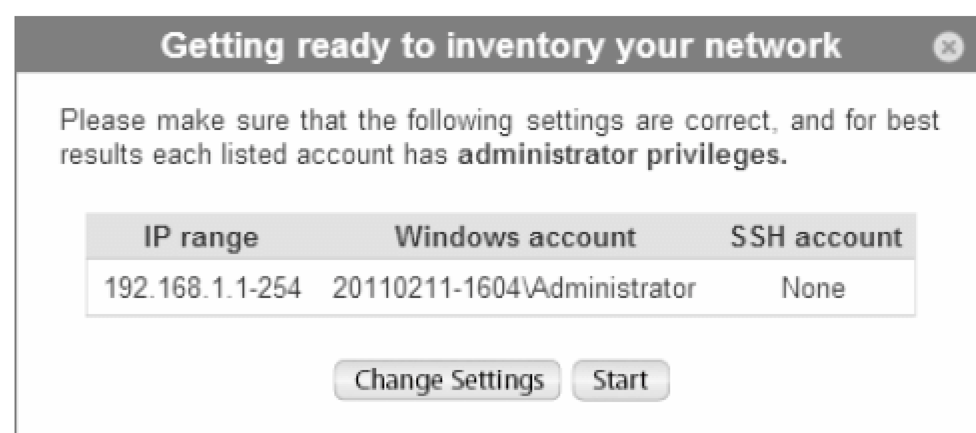


图 17-19　Getting ready to inventory your network 页面

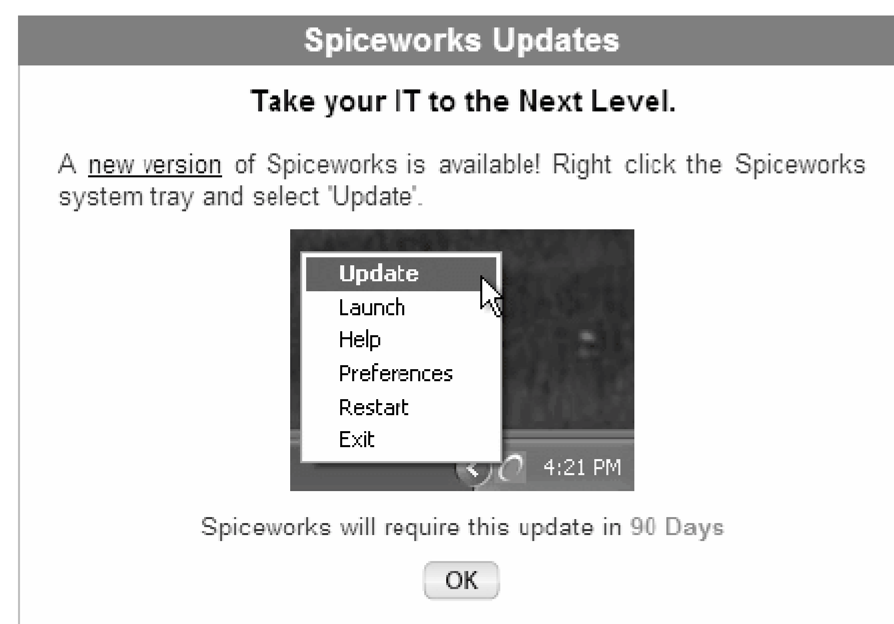


图 17-20　Spiceworks Updates 页面

07 系统进入扫描页面，自动对“192.168.1.1-254”网段的所有设备进行扫描，如图 17-21 所示。

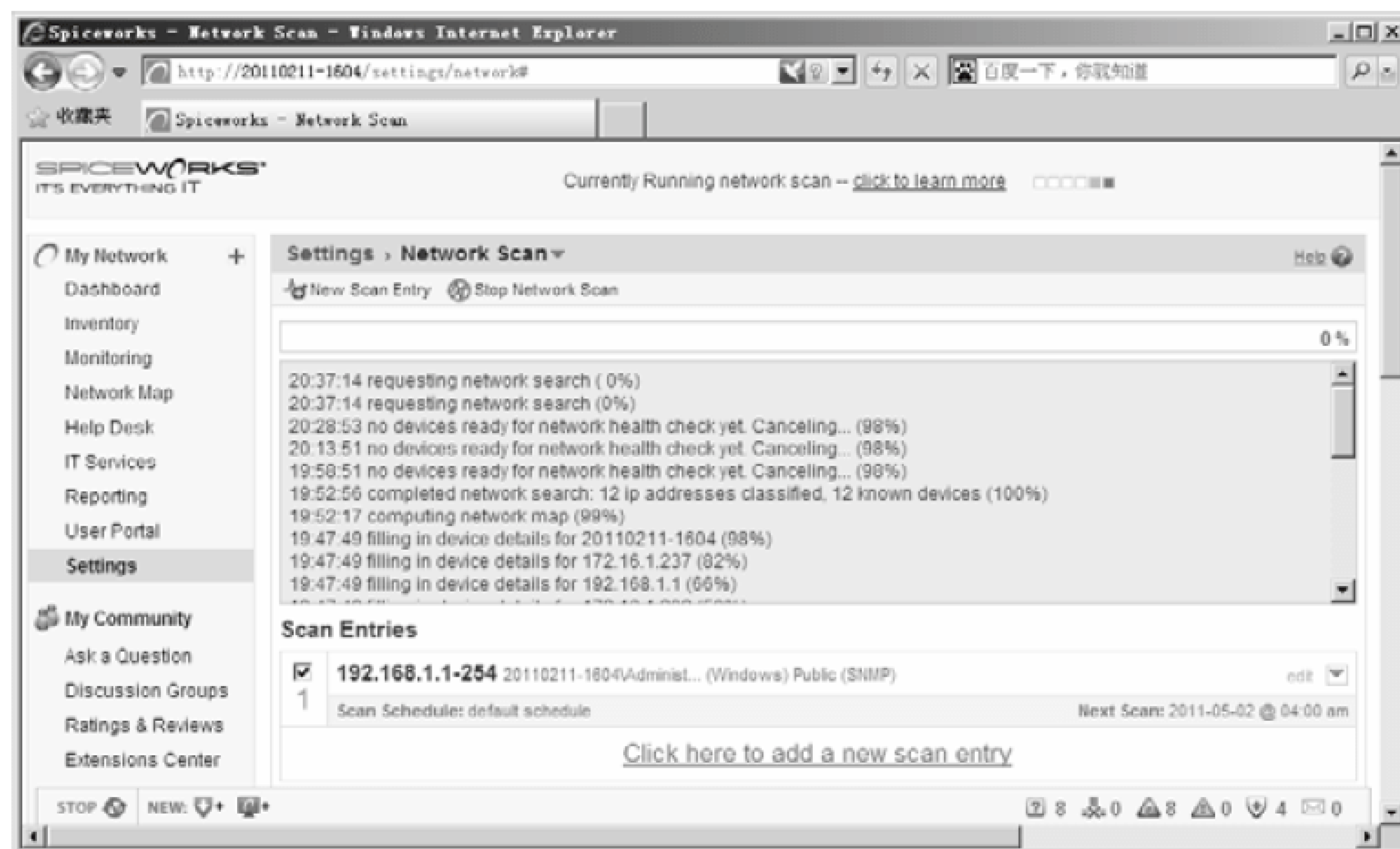


图17-21　程序扫描目标网络设备

3. 扫描指定网段的网络拓扑结构

默认情况下，Spicework 只对服务器所在网段的设备扫描，如果需要扫描其他网段必须手工设置。

本实例以扫描范围“172.16.1.1-254”为例讲述如何手动设置，具体操作步骤如下。

01 在 Getting ready to inventory your network 页面中，单击 Change Settings（改变设置）按钮。

02 进入扫描网络设置页面，单击 Click here to add a new scan entry（单击这里添加新扫描网络）超级链接，如图 17-22 所示。

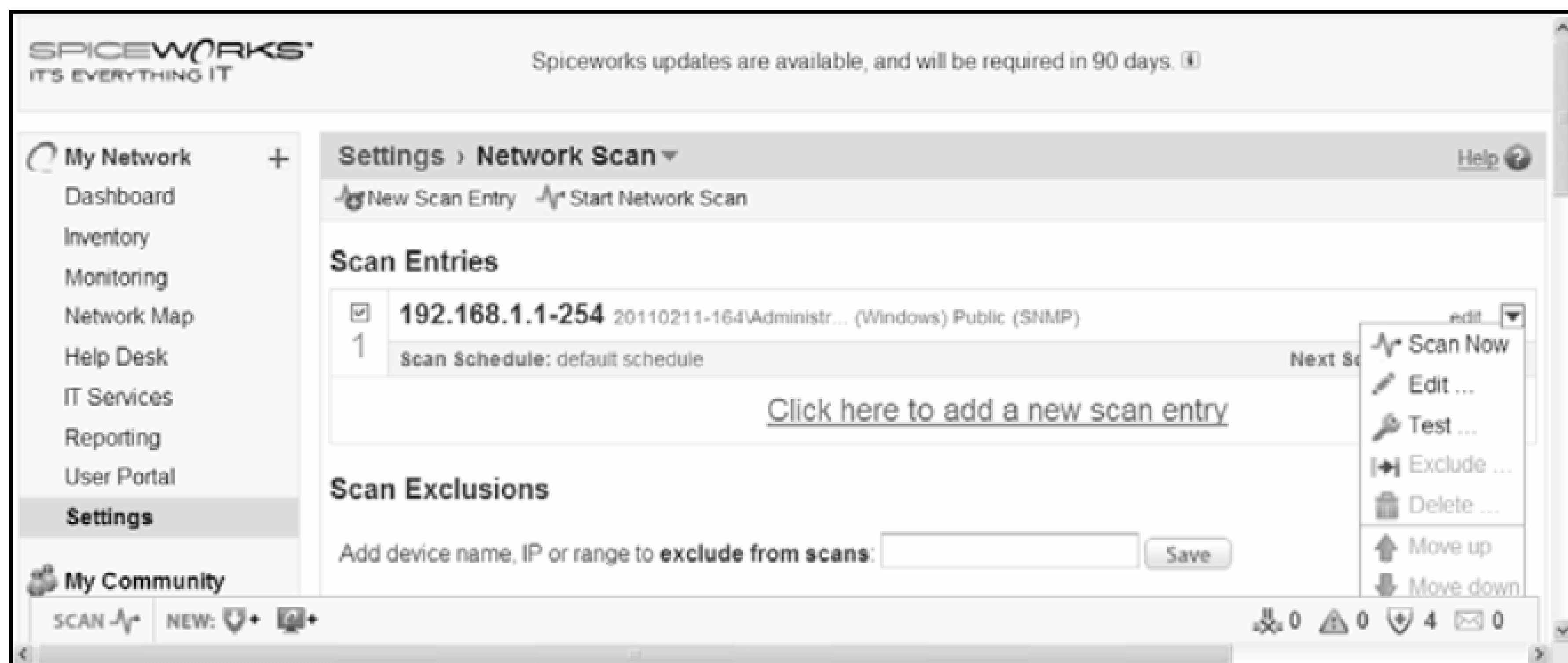


图 17-22　扫描网络设置页面

03 弹出 Add New Scan Entry（添加新扫描网络）页面，在 Device/Range（设备或组）文本框中输入扫描范围“172.16.1.1-254”，在该文本框还可输入区域名，如图 17-23 所示。

04 在 SNMP 文本框中选择 Public 为 SNMP 协议的团体名（也可根据实际情况单击 add new SNMP account（添加新 SNMP 清单）超级链接，添加新的团体名），单击 Save 按钮，如图 17-24 所示。

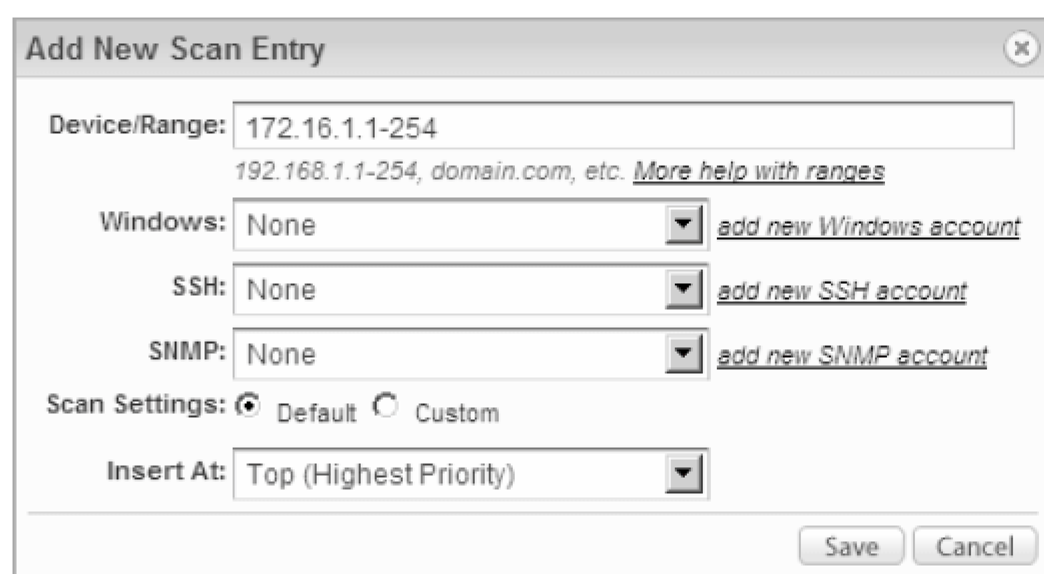


图 17-23　Add New Scan Entry 页面

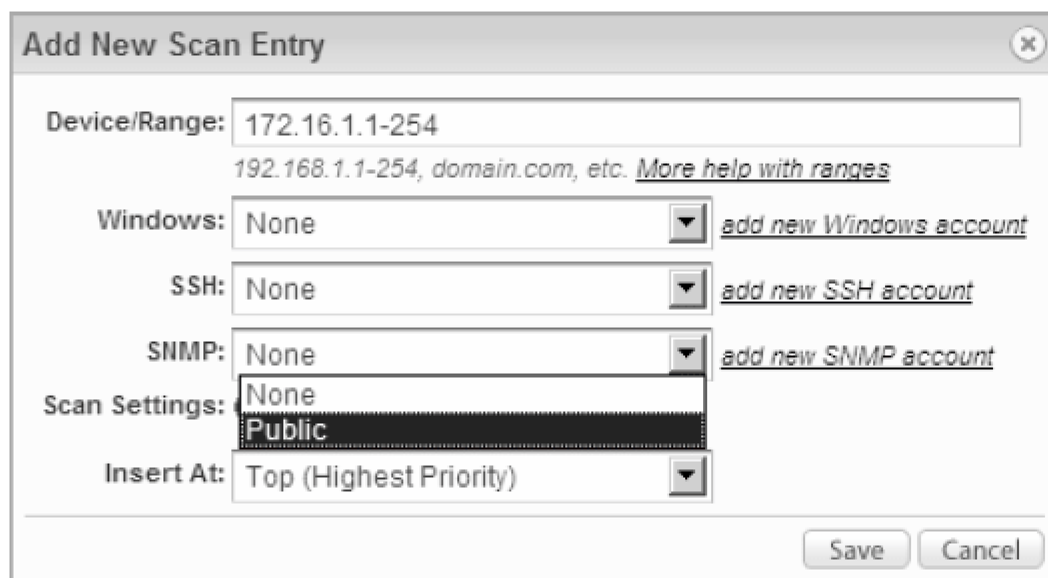


图 17-24　配置网络管理协议

05 新扫描范围添加成功，选择全部扫描范围，单击 Start Network Scan 超级链接，如图 17-25 所示。

06 弹出 Getting ready to inventory your network 页面，单击 Start 按钮即可开始扫描自定义的网络，如图 17-26 所示。

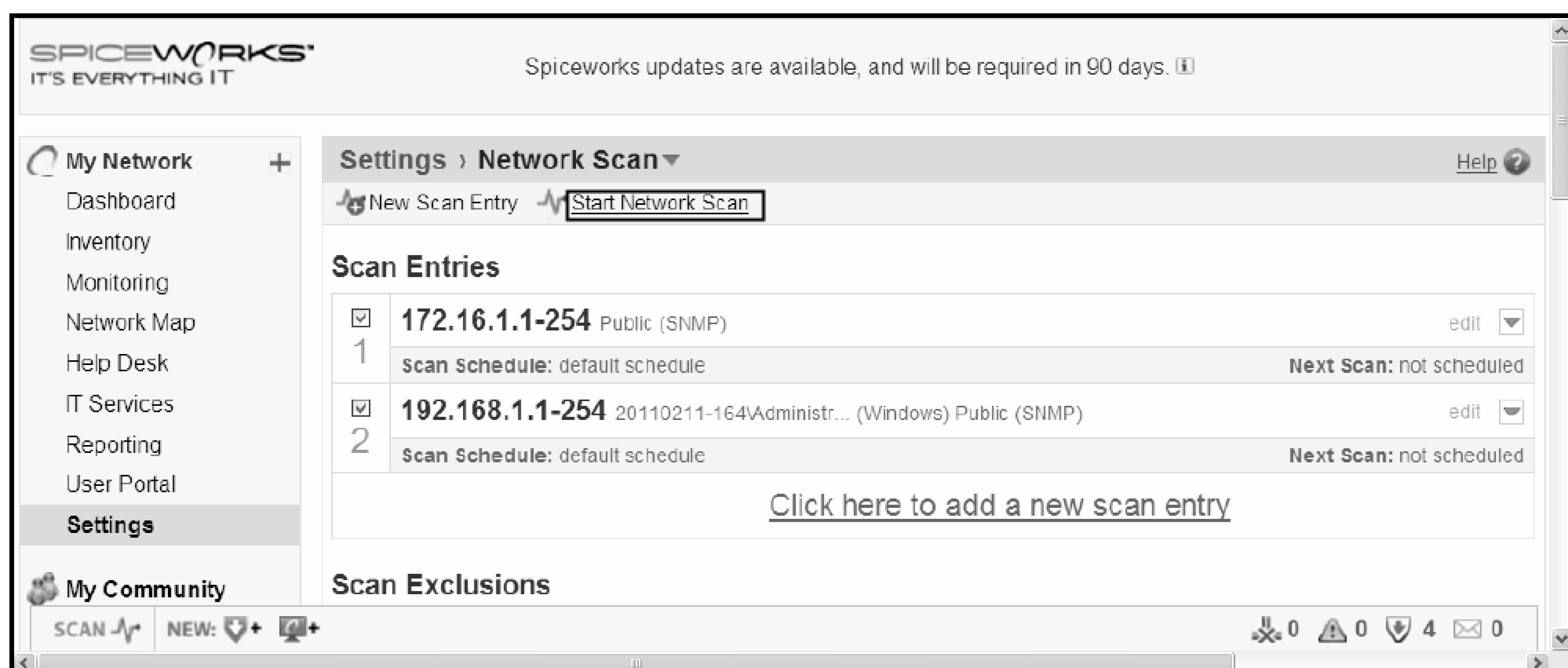


图 17-25　成功添加网络扫描范围

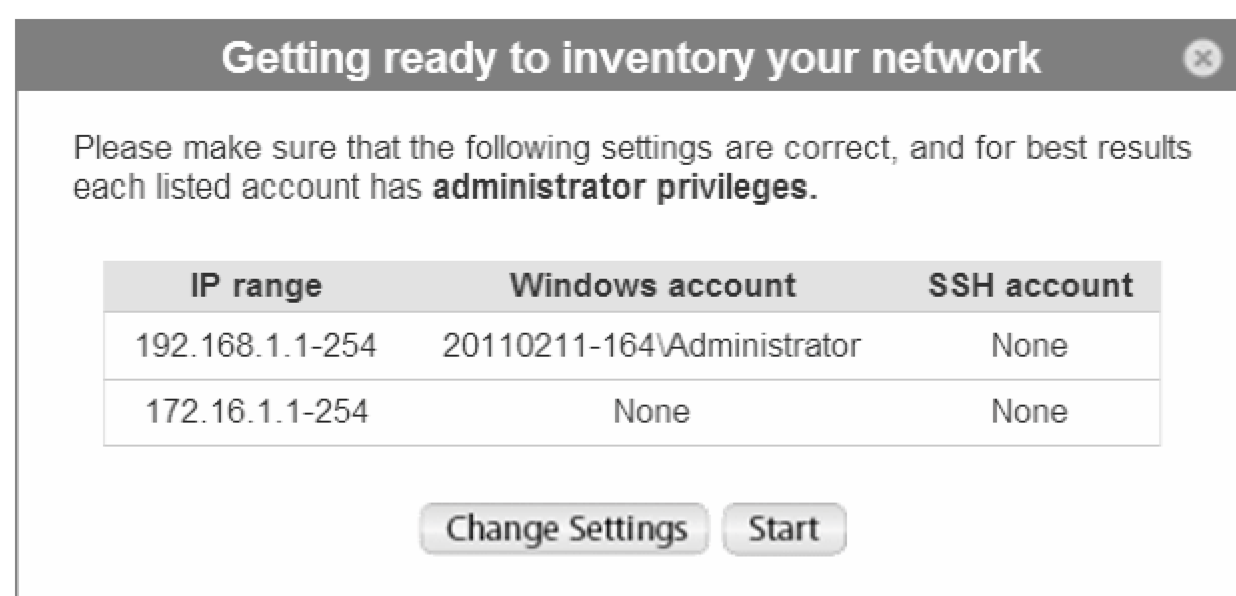


图 17-26　开始扫描网络

4．通过 Network Map 模块查看网络拓扑及信息

网络扫描结束后，需清晰直观地查看网络信息，可以使用 Spiceworks 网络管理平台提供的 Network Map 模块。

使用 Network Map 模块的具体操作步骤如下。

01 在 Spiceworks 主界面的左侧选项列表中选择 Network Map（网络地图）选项，在页面右侧窗格中显示出扫描后的网络拓扑图，拓扑图中每一个图标代表一个设备。可以通过图形缩放、移动工具调整拓扑图大小及位置，也可以通过鼠标单击拖曳或滑轮改变拓扑布局及大小，如图 17-27 所示。

02 软件默认为 Hierarchy Layout（分层布局）模式。选择 Arrange（布局）➢ Radial Layout（放射状）命令，改变网络拓扑图显示方式，如图 17-28 所示。

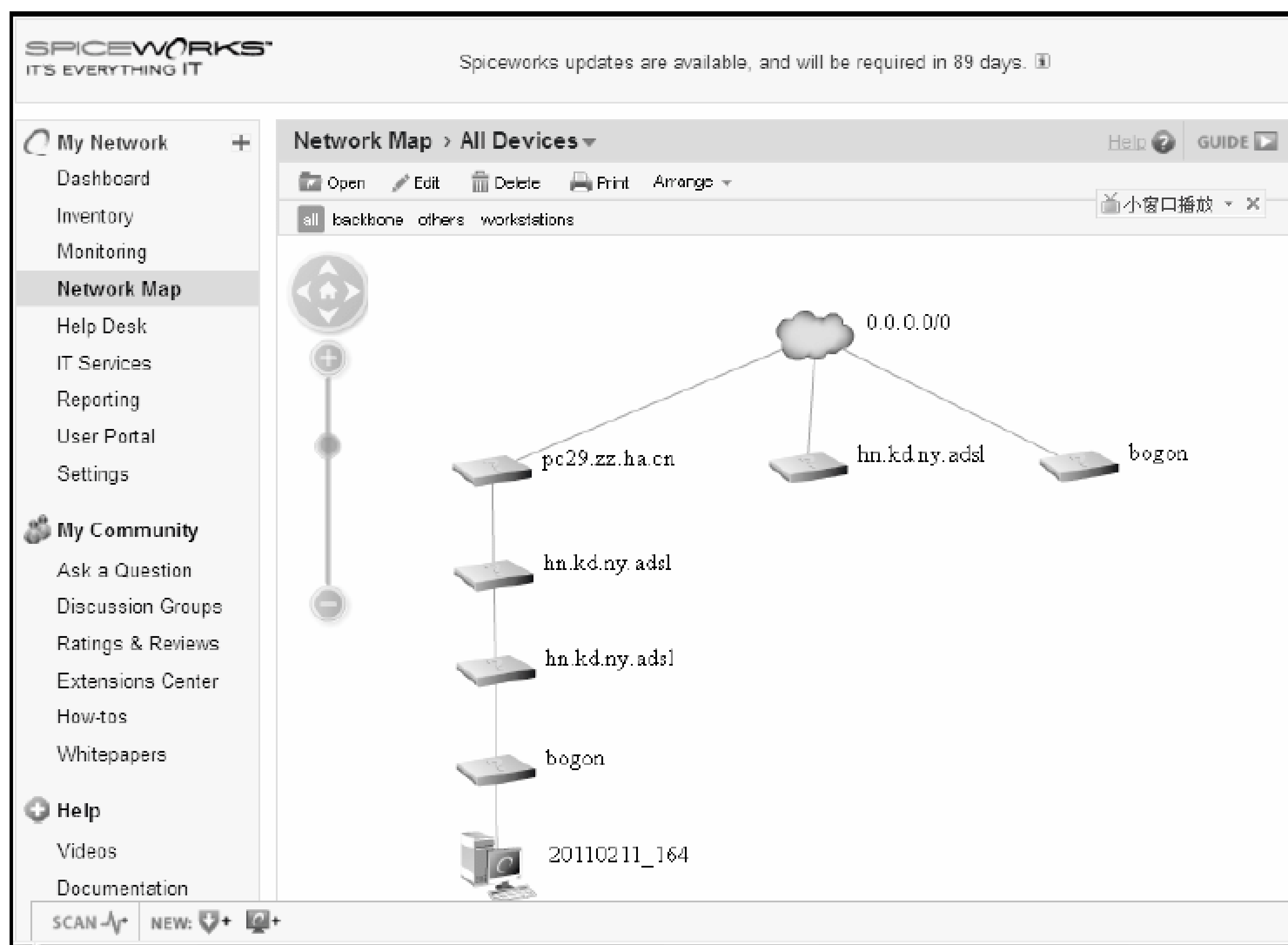


图 17-27　Spiceworks 主界面

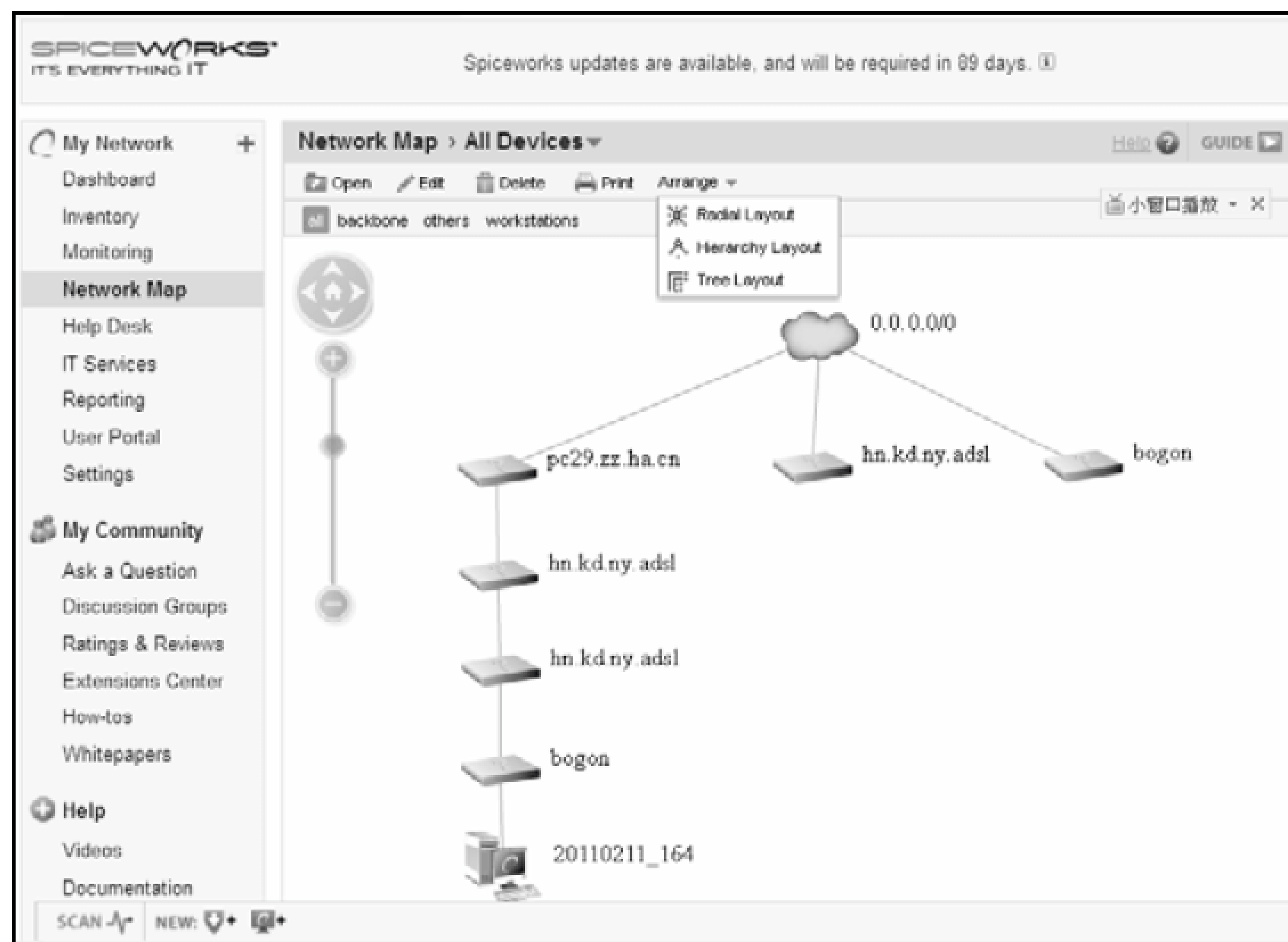


图 17-28　Network Map 选项

03 改变后的拓扑图模式，表现为放射状，如图 17-29 所示。

04 单击网络设备的图标并拖曳到适当的位置，将网络拓扑图调整得更加直观，如图 17-30 所示。

05 单击想要查看的设备图标，弹出该设备的摘要信息框，如图 17-31 所示。

06 单击 Edit 按钮，打开网络拓扑图编辑页面，在该页面也可以调整网络拓扑图，调整完成之后，单击 Save 按钮，如图 17-32 所示。

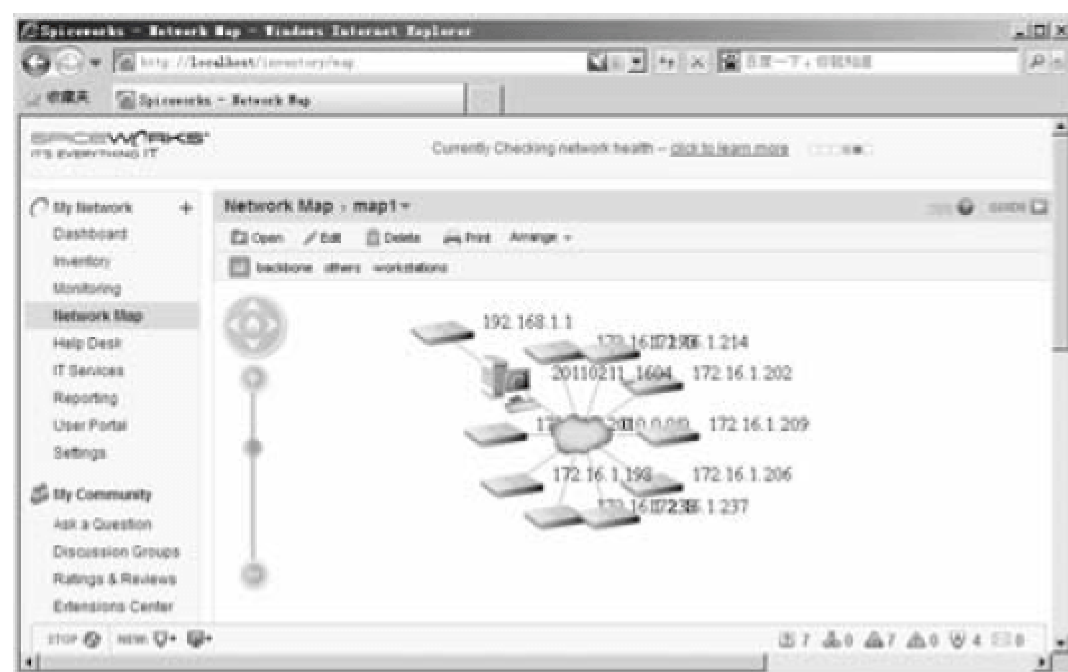


图 17-29　放射状网络拓扑图

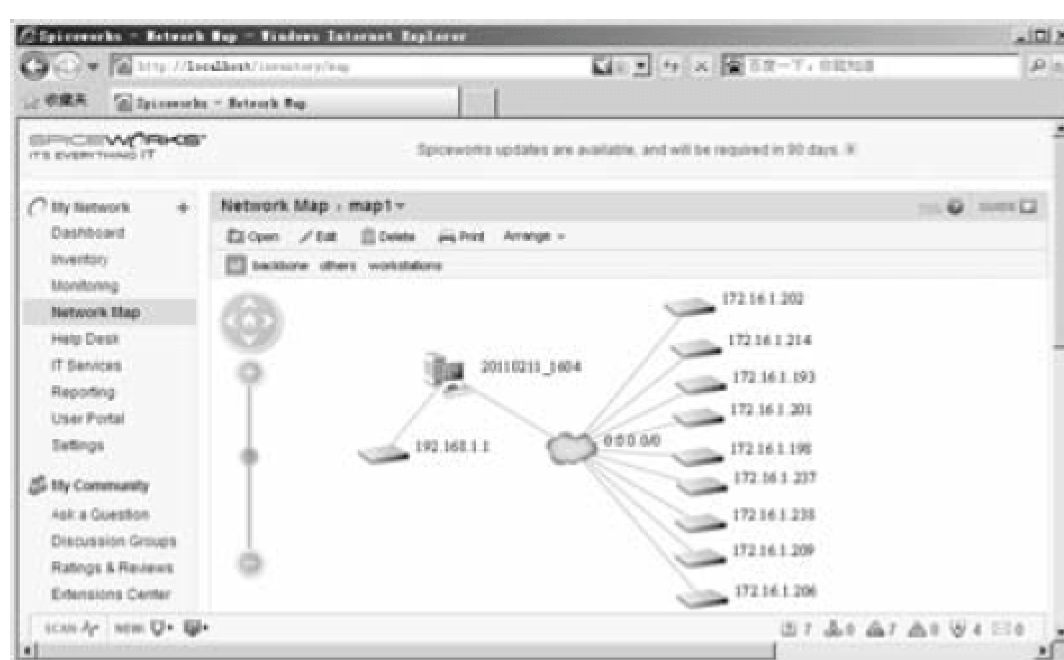


图 17-30　调整网络拓扑图

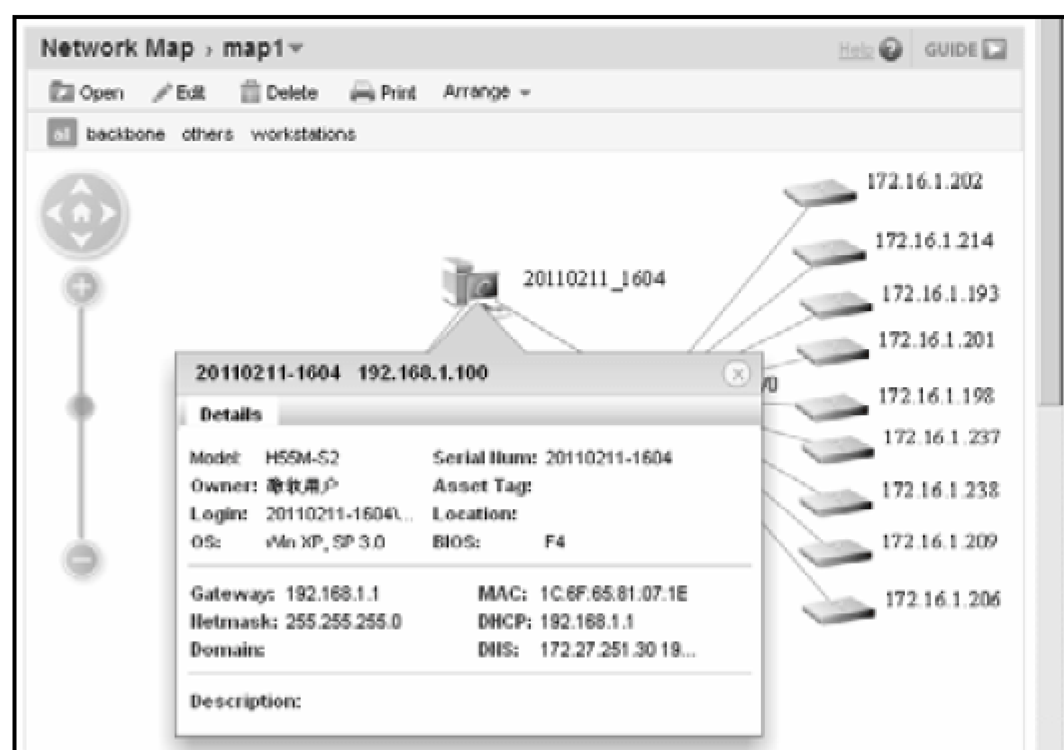


图 17-31　查看设备摘要信息

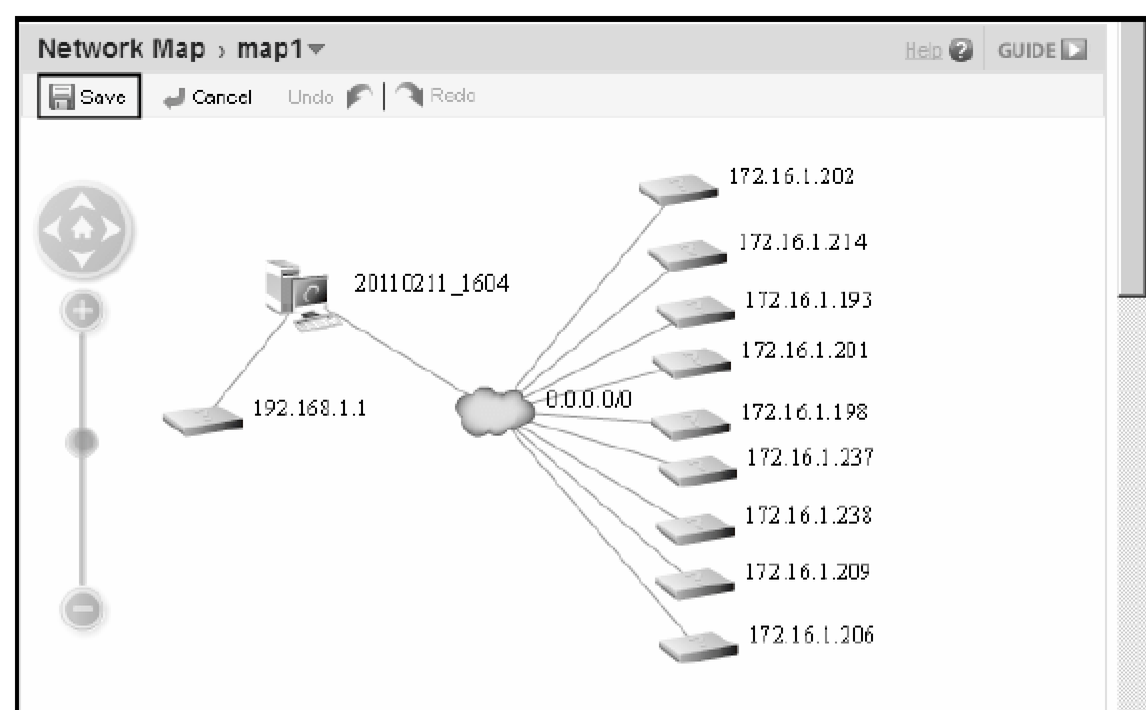


图 17-32　编辑保存网络拓扑图

07 弹出 Save the map（保存地图）页面，单击 Save new（保存新名）按钮，如图 17-33 所示。

08 在 Map name（地图名字）文本框中输入网络拓扑图的名称（可用时间、范围等信息作为网络拓扑图名称，以方便记忆、查询），单击 Save 按钮，如图 17-34 所示。

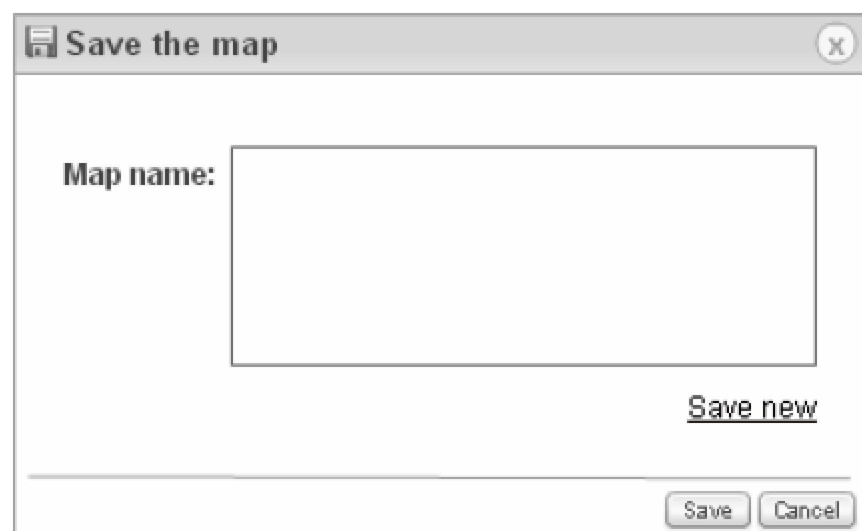


图 17-33　Save the map 页面

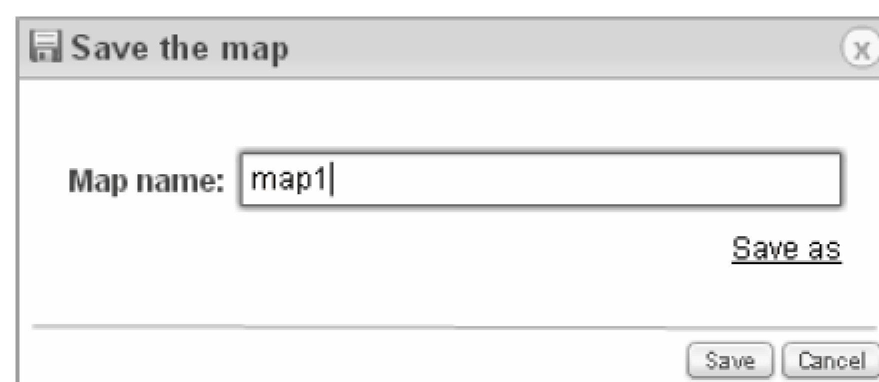


图 17-34　配置 Map name

09 返回到软件主界面，单击 Open 按钮，如图 17-35 所示。

10 弹出 Open a map（打开一个地图）页面，选中网络拓扑图名，单击 Open 按钮即可打开选中的网络模块，如图 17-36 所示。

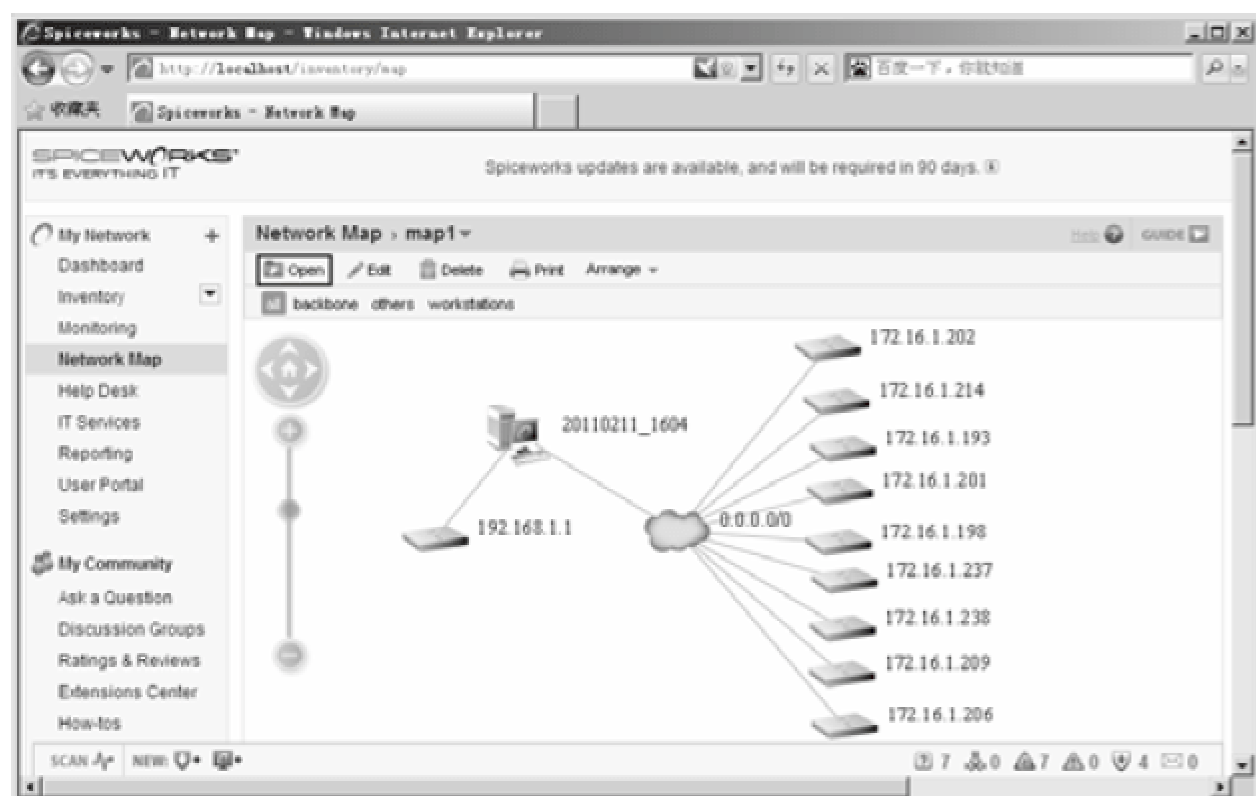


图 17-35 单击 Open 按钮打开已保存拓扑图

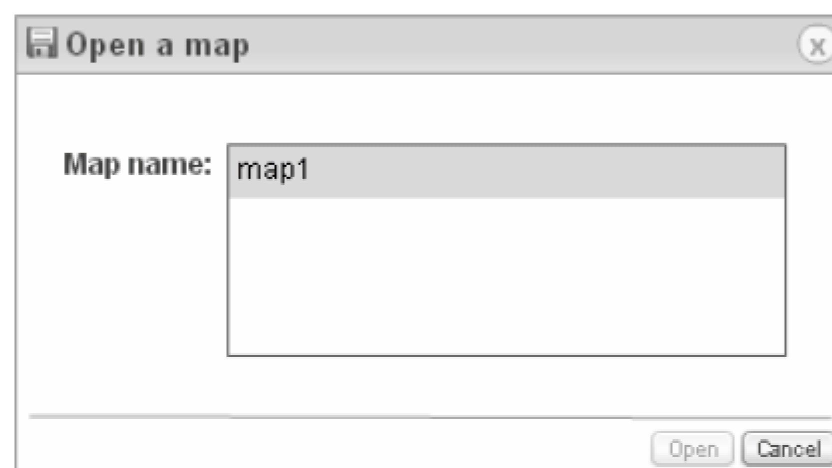


图 17-36 Open a map 页面

17.2.3 应用网管平台

Spiceworks 软件的管理功能比较多，如设备信息查看、管理日志、仪表盘快速浏览管理信息等。下面介绍几种常用的功能。

1. 设置 Spiceworks 仪表盘，直观高效地查看网络管理信息

为了方便多种管理信息的查看，Spiceworks 设定了仪表盘模块，具体操作步骤如下。

01 在 Spiceworks 主界面的左侧选项列表中选择 Dashboard（仪表板）选项，如图 17-37 所示。

02 在弹出的页面中单击 Add Content（添加模块）超级链接，弹出 Add Content 模块选项列表，单击需要显示的模块的超级链接，即可添加模块到仪表盘页面，如图 17-38 所示。

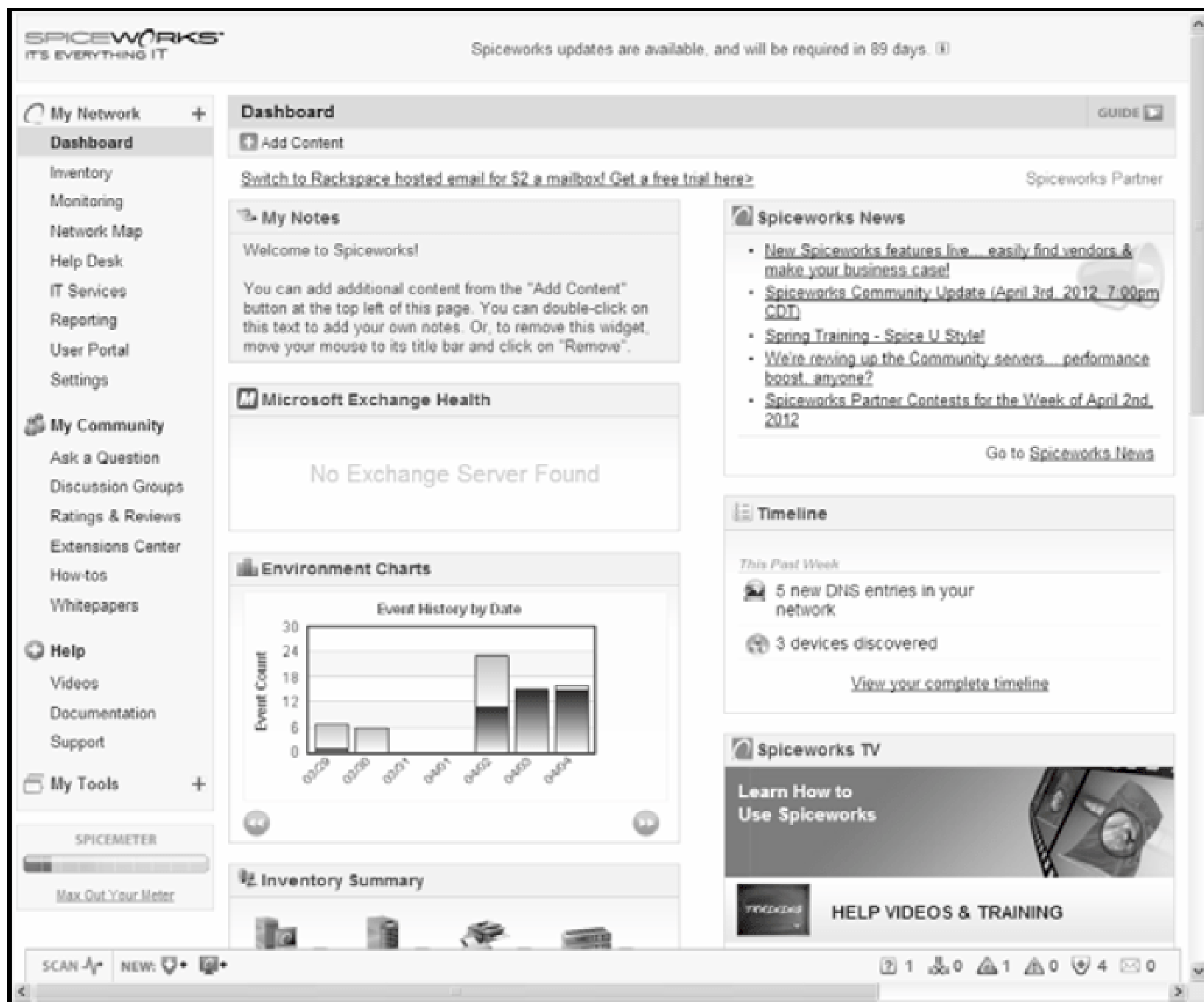


图 17-37 Spiceworks 程序主界面

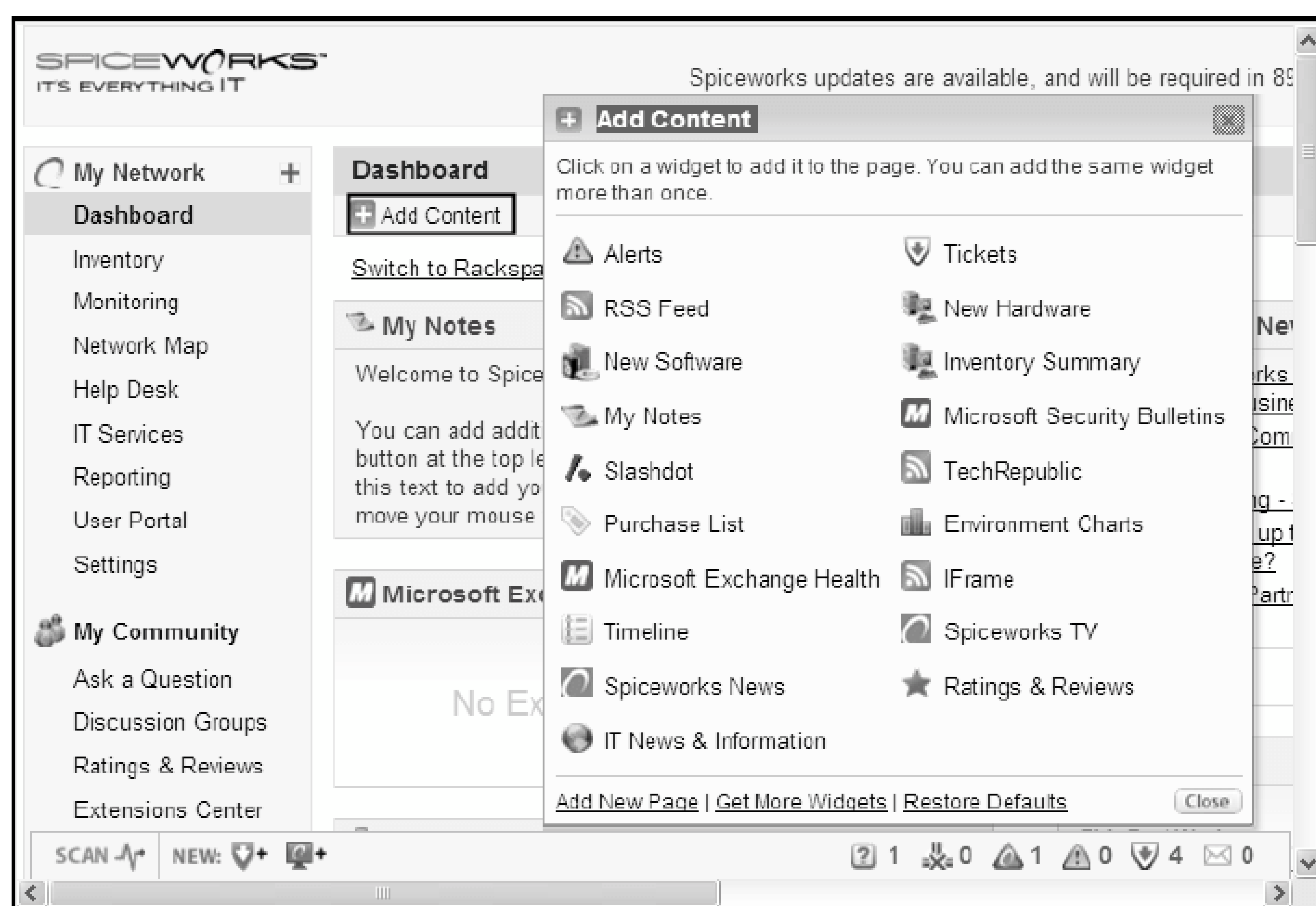


图 17-38　Add Content 模块

仪表盘中的显示模块比较多，常用模块的功能介绍如下。

- Alerts（告警）：告警模块，显示最近发生的告警信息。
- New Hardware（新硬件）：新硬件模块，显示新加网络设备。
- New Software（新软件）：新软件模块，显示新安装的软件信息。
- Inventory Summary（存货清单摘要）：设备信息摘要模块，显示现有设备。
- My Notes（我的日志）：日志模块，查看、编辑日志。
- Microsoft Security Bulletins（微软安全公告）：微软安全公告模块，显示微软发布的安全公告信息。
- Timeline（大事年表）：事件记录模块，显示 Spiceworks 网络管理平台最近发生的事件。
- IT News & Information（IT 新闻和消息）：业界新闻消息模块。

03　单击 Remove（移除）链接，可以移除指定模块，如图 17-39 所示。

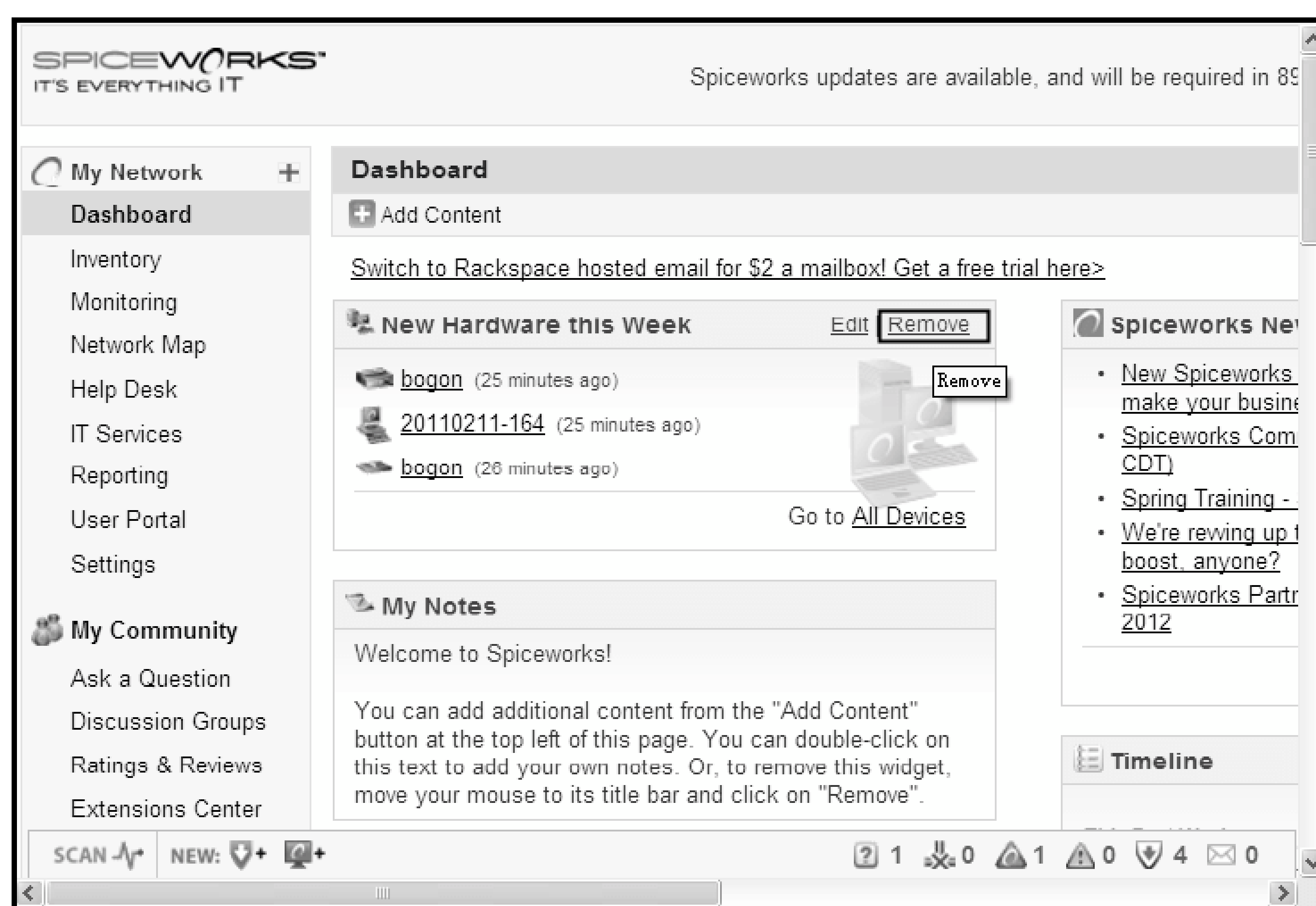


图 17-39　移除模块

2. 使用 Inventory 设备清单模块，查看设备详细信息

通过 Inventory 模块，可以查看设备的详细信息，具体操作步骤如下。

01 在 Spiceworks 主界面的左侧选项列表中选择 Inventory（库存清单）选项，右侧窗格中显示出已有设备清单。如果要查看某一设备的详细信息，可以进入该设备的类别中进行查看，本实例通过查看某主机设备的信息为例进行讲解，单击 Workstations（工作站）对象类别图标，如图 17-40 所示。

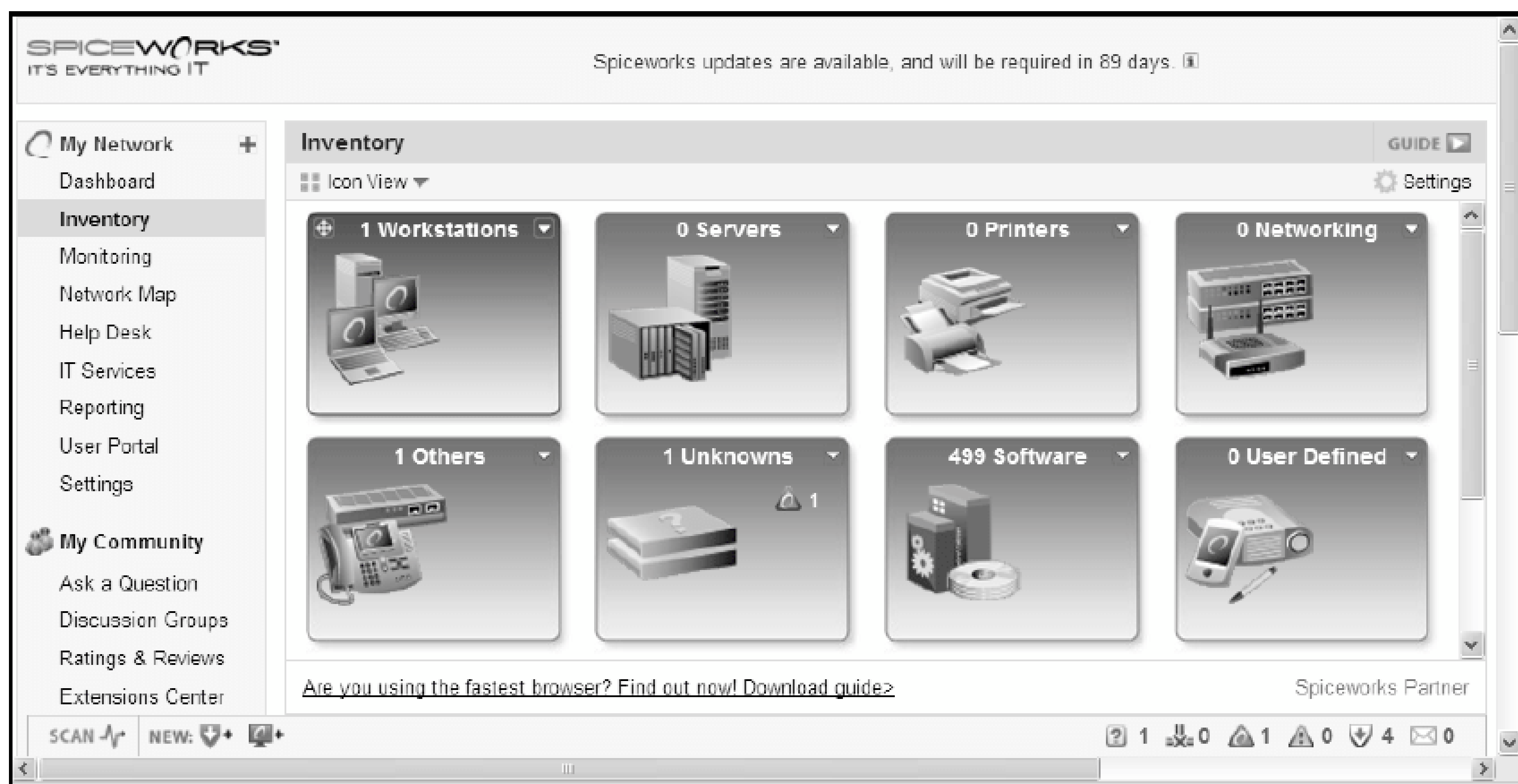


图 17-40　Inventory 选项

02 在右侧窗格中显示 Workstations 对象类别的设备列表，单击要查看的主机设备图标，显示该设备的详细信息，如图 17-41 所示。

03 在页面的下方显示出对象的详细信息，默认显示 General Info（常规信息）选项卡，如图 17-42 所示。

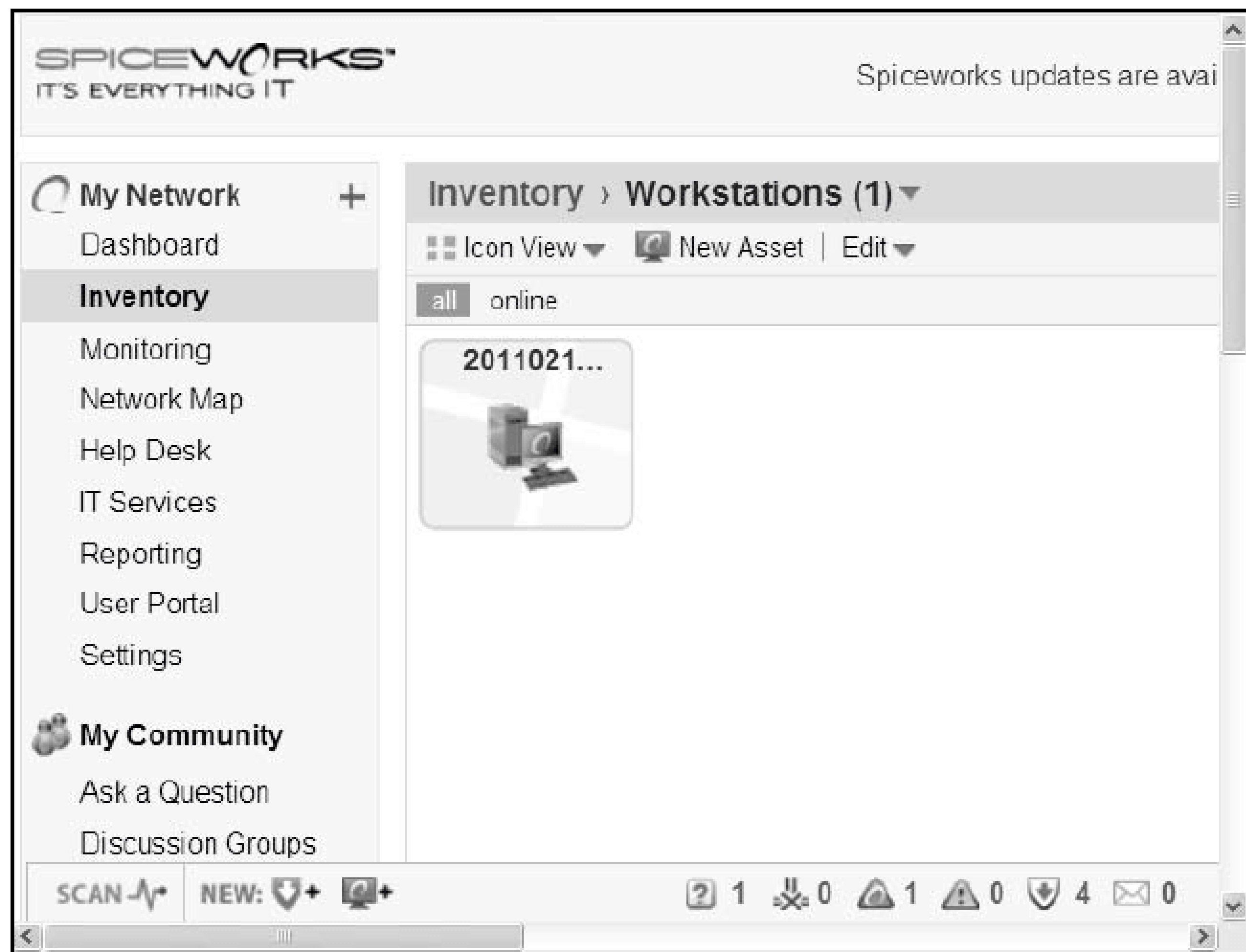


图 17-41　查看设备详细信息

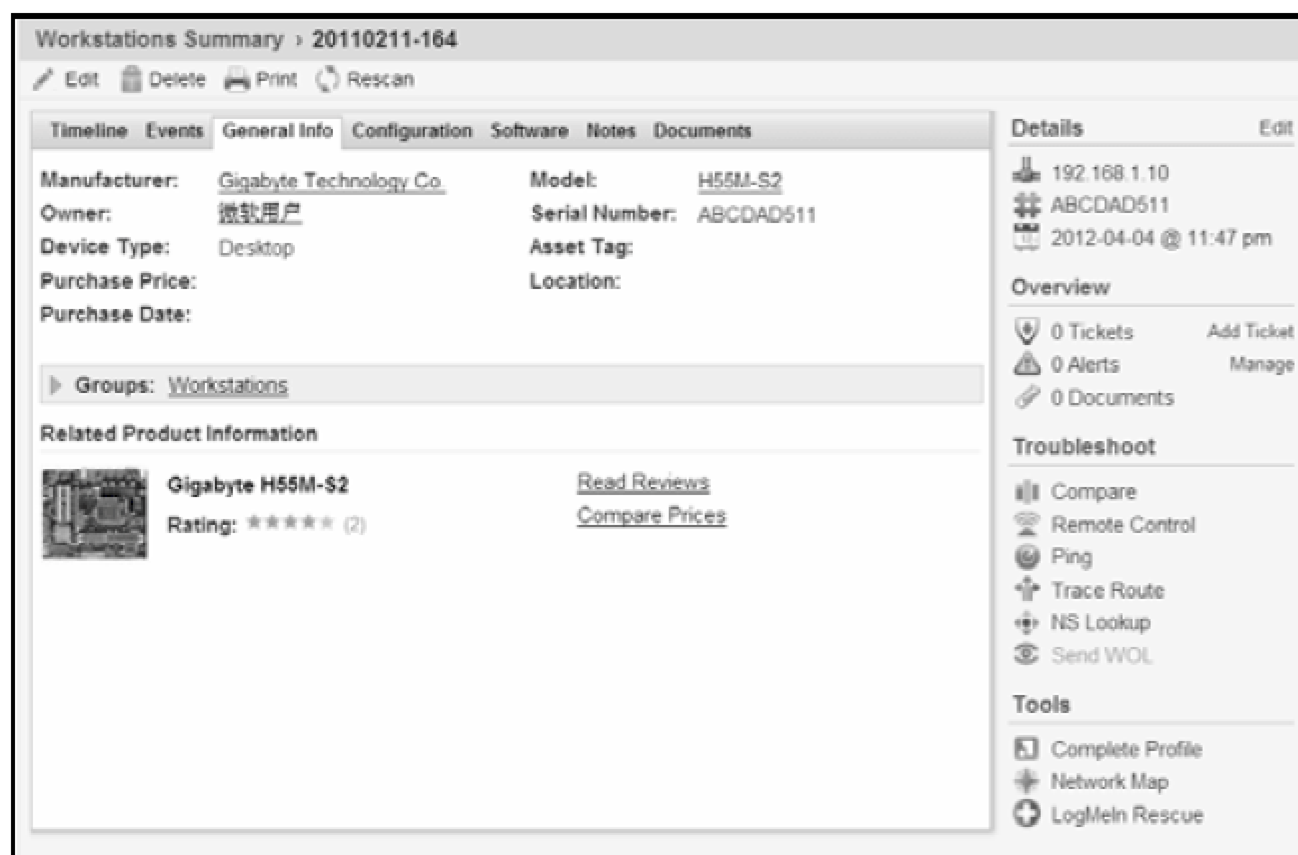


图 17-42　General Info 选项卡

04 选择 Timeline（大事年表）选项卡，查看该对象的操作记录，如图 17-43 所示。

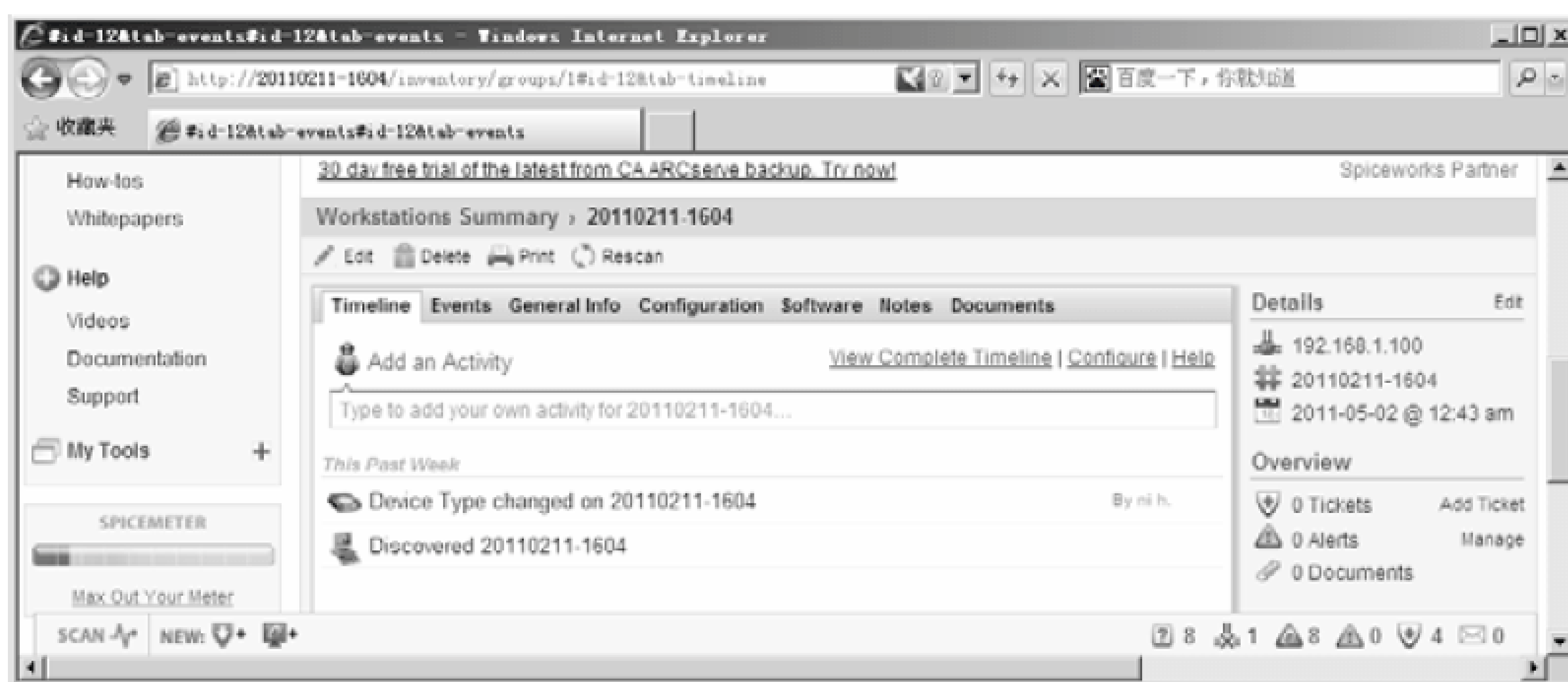


图 17-43　Timeline 选项卡

05 选择 Events（事件）选项卡，查看该对象的事件记录信息，如图 17-44 所示。

06 选择 Configuration（配置）选项卡，查看该对象的配置信息，如图 17-45 所示。

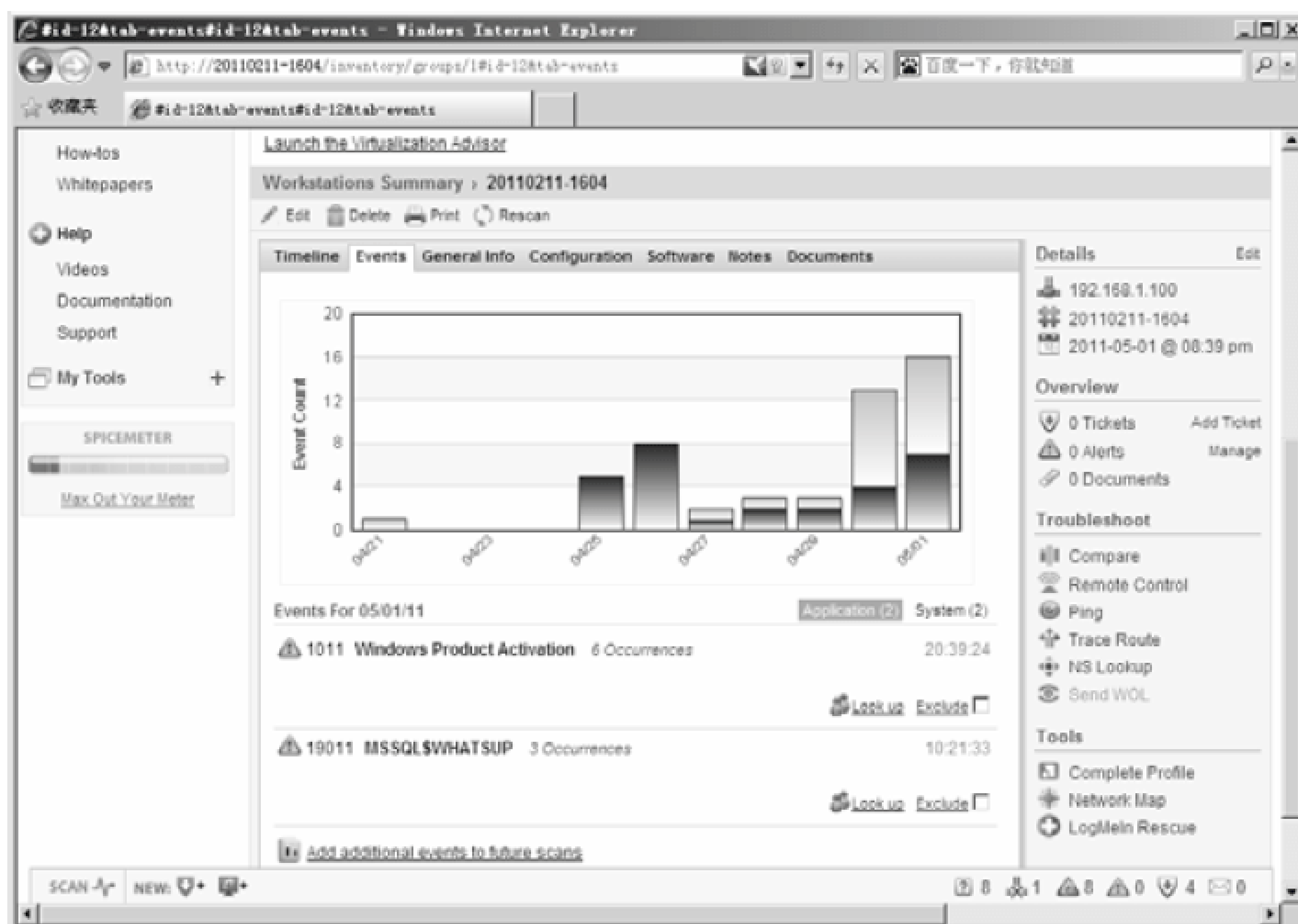


图 17-44　Events 选项卡

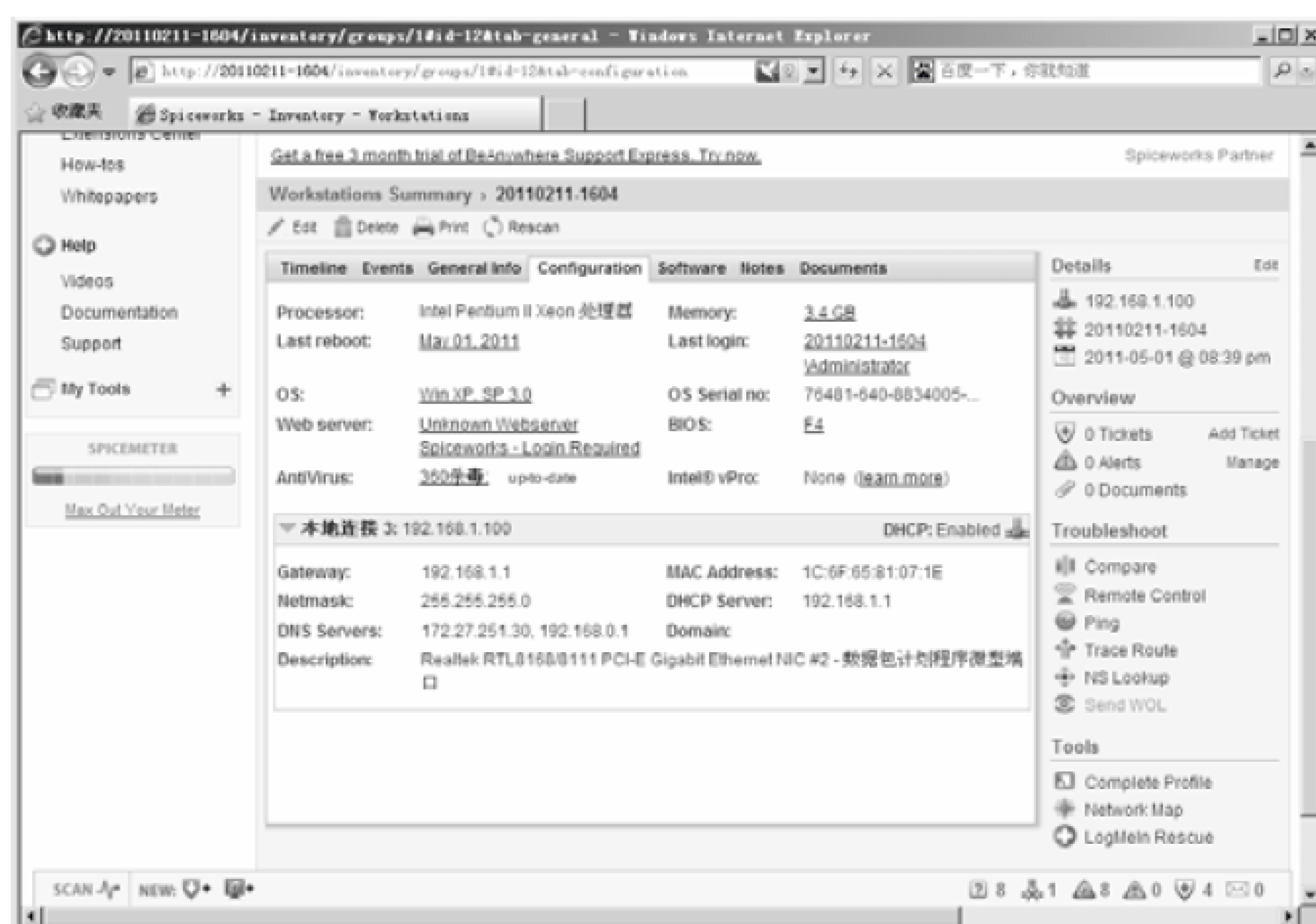


图 17-45　Configuration 选项卡

07 选择 Software 选项卡，查看该主机安装的软件信息，单击 Edit 按钮，如图 17-46 所示。

08 进入对象编辑界面，可以编辑该对象的部分信息，如图 17-47 所示。

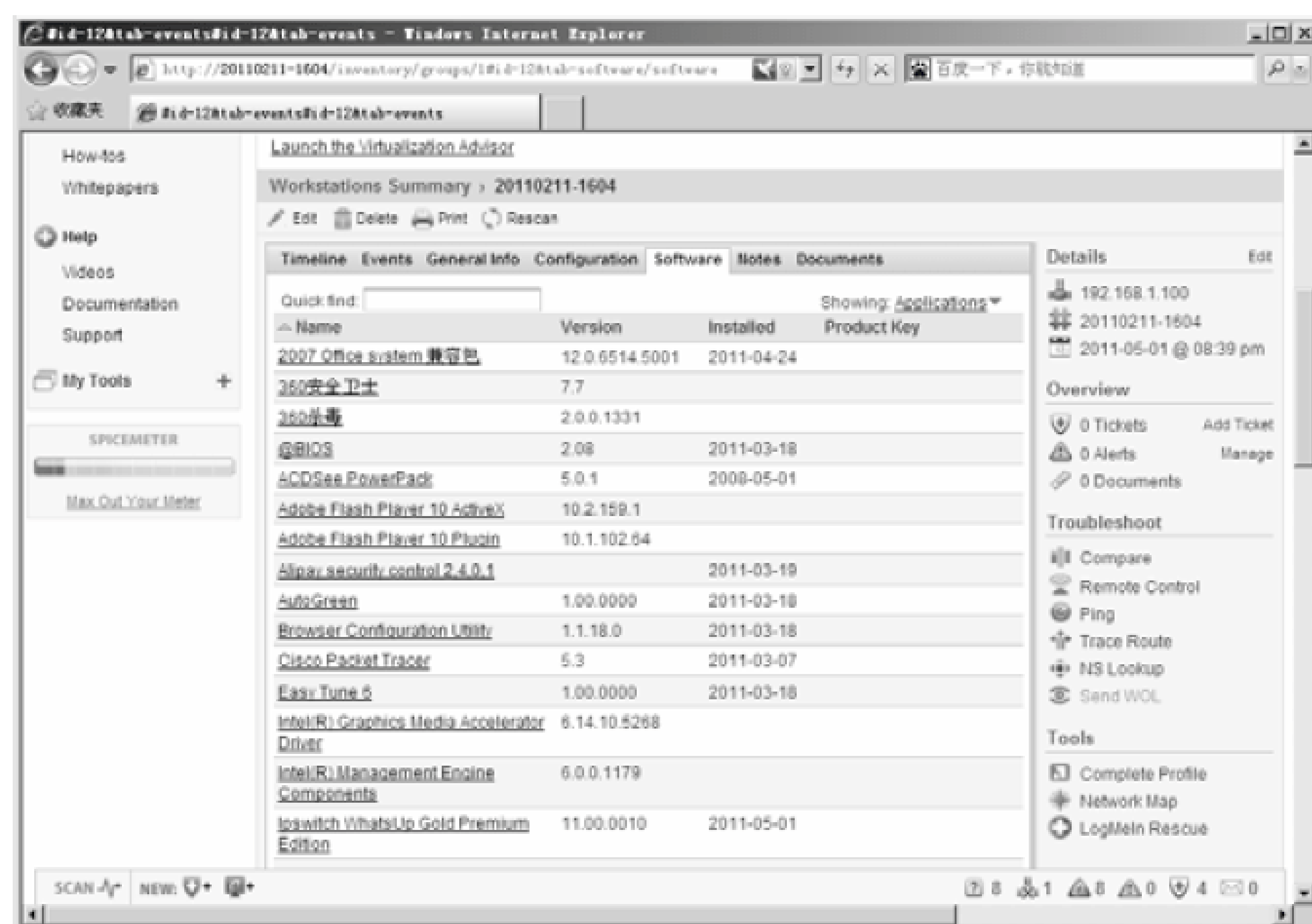


图 17-46　Software 选项卡

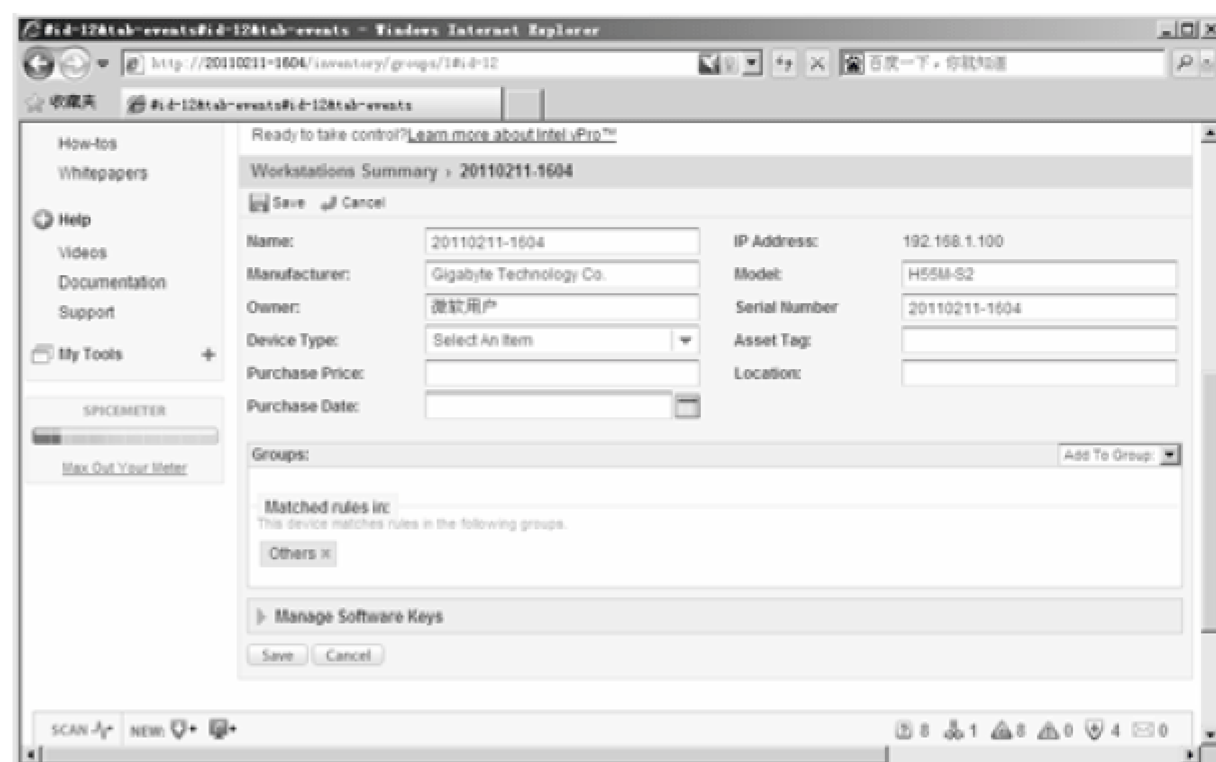


图 17-47　对象信息编辑界面

信息查看还有另一种界面可选，具体操作步骤介绍如下。

01 选择 Icon View（图示视图）➢Browse View（浏览视图）命令，如图 17-48 所示。



图 17-48　选择 Browse View 方式查看设备信息

02 进入对象信息显示界面，可以查看对象的详细参数信息，如图 17-49 所示。

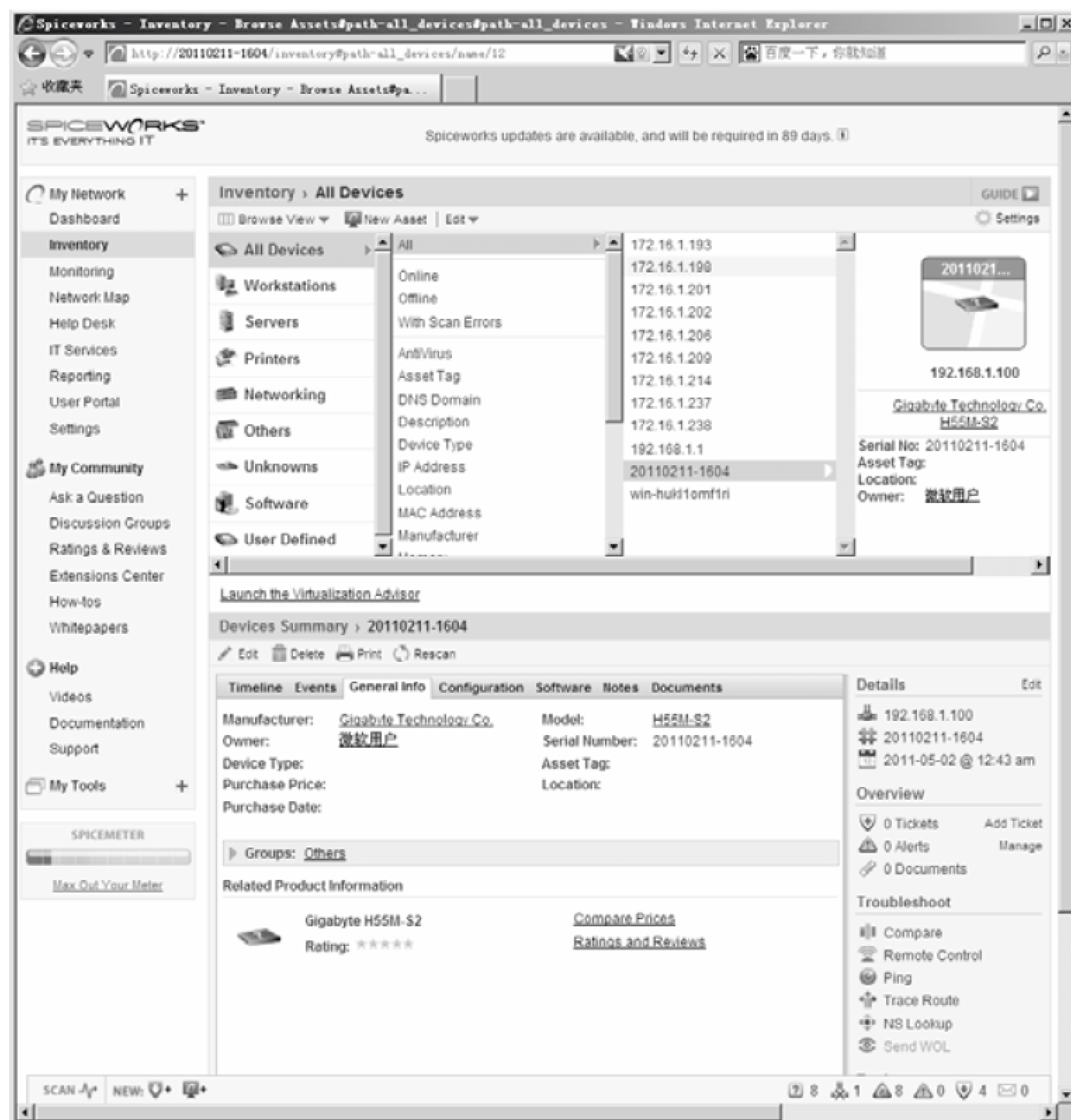


图 17-49　Browse View 对象信息查看界面

3. 扫描新添加的网络

在网络中有新用户或新网络添加时，需及时对新添加的设备或网段进行扫描，具体操作步骤如下。

01 选择 Spiceworks 界面左侧选项列表中的 Settings 选项，并单击右侧窗口中的 Network Scan（网络扫描）图标，如图 17-50 所示。



图 17-50　Settings 界面

02 进入 Network Scan 界面，单击 Click here to add a new scan entry 链接，添加新网络并进行扫描，如图 17-51 所示。

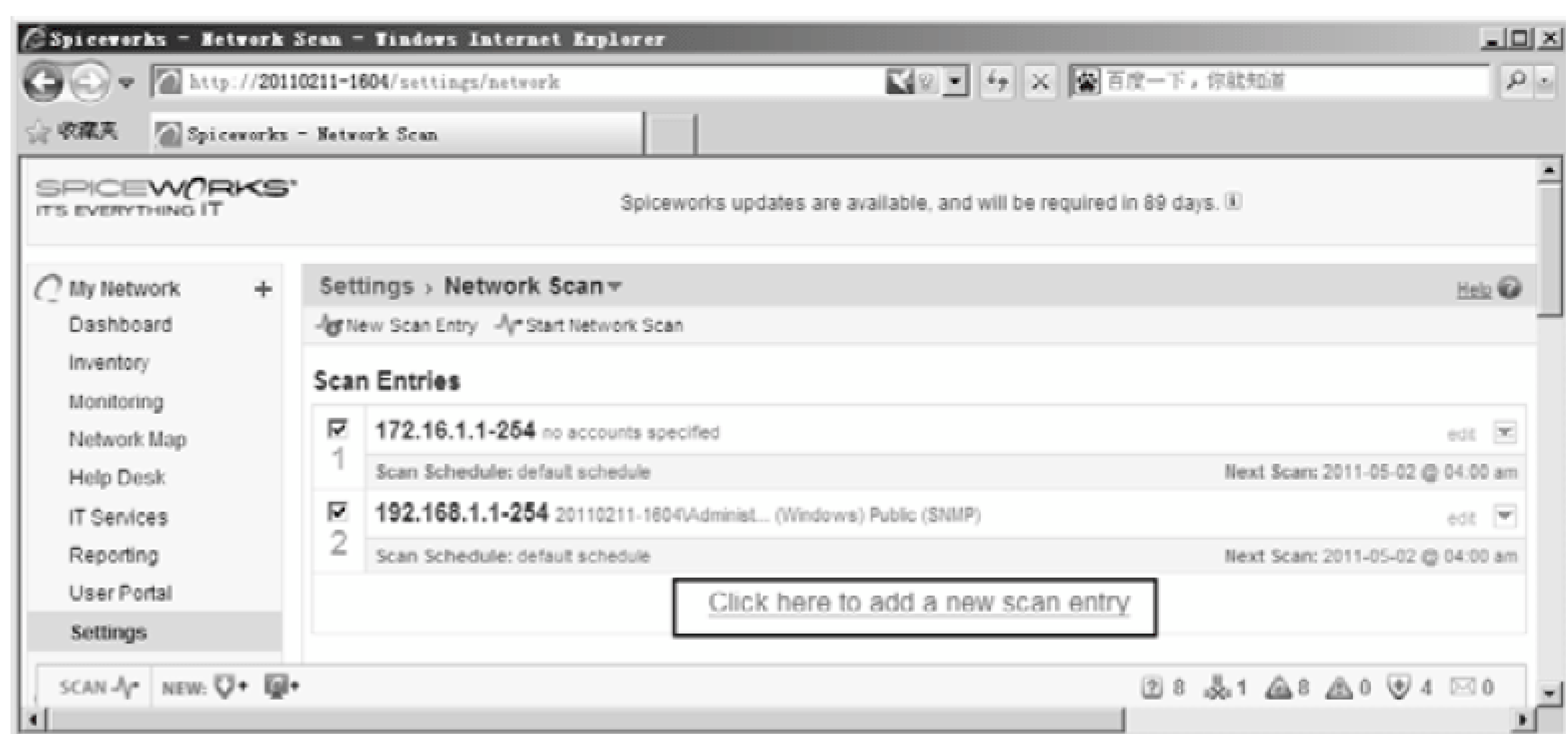


图 17-51　Network Scan 界面

17.3　项目实战 2：搭建 WhatsUp Gold 网络管理平台

WhatsUp Gold 软件也是一款功能完善的网络管理软件，它与 Spiceworks 软件的功能及实现流程相似。下面主要介绍 WhatsUp Gold 网络管理平台的搭建及应用方法。

17.3.1　架设网络管理平台

WhatsUp Gold 与 Spiceworks 的环境要求相似，但是具体的操作方法不同。安装 WhatsUp Gold 的具体操作步骤如下。

01 运行安装程序，弹出 Welcome 对话框，单击 Next 按钮，如图 17-52 所示。

02 弹出 License Agreement 对话框，选择 I accept the terms of the license agreement（接受许可协议）复选框，单击 Next 按钮，如图 17-53 所示。



图 17-52　Welcome 对话框



图 17-53　License Agreement 对话框

03 弹出 Enter MSDE-2000 Server Paths（Mictosoft 数据库服务器路径）对话框，单击 Browse 按钮，可以设置数据库文件存放的位置，本实例采用默认配置，单击 Next 按钮，如图 17-54 所示。

04 弹出 Choose Destination Location(更改目录位置)对话框，单击 Browse 按钮，可以设置 WhatsUp Gold 软件的安装目录位置，本实例采用默认配置，单击 Next 按钮，如图 17-55 所示。



图 17-54　Enter MSDE-2000 Server Paths 对话框



图 17-55　更改安装目录位置

05 弹出 Enable Web Server（设置 Web 服务）对话框，选中 Yes 复选框，开启 WhatsUp Gold 服务器的 Web 访问功能，在 Enable Web server on port(设置 Web 服务端口)文本框中输入 Web 连接端口，本实例采用默认配置“80”端口，单击 Next 按钮，如图 17-56 所示。

06 弹出 Ready to Install the Program（准备安装程序）对话框，单击 Install 按钮，如图 17-57 所示。

07 系统开始自动安装 WhatsUp Gold，并显示安装的进度，如图 17-58 所示。

08 WhatsUp Gold 安装完成后，单击 Finish 按钮，如图 17-59 所示。

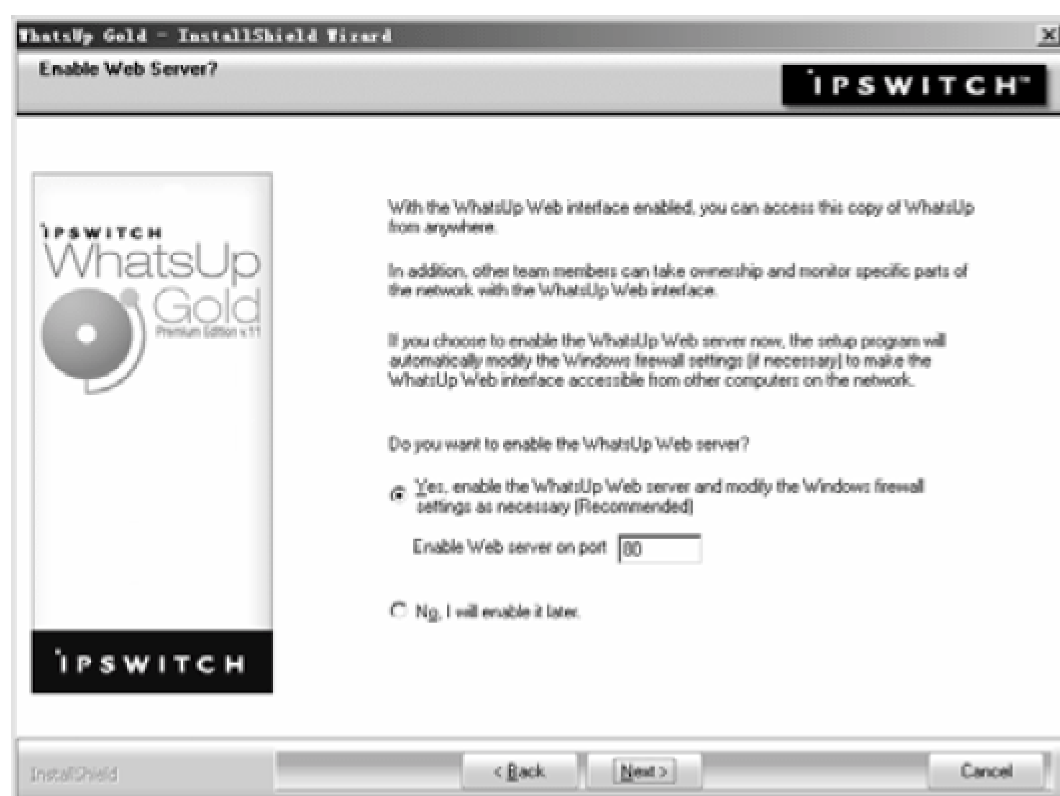


图 17-56　Enable Web　Server 对话框



图 17-57　Ready to Install the Program 对话框



图 17-58　系统自动安装 WhatsUp Gold

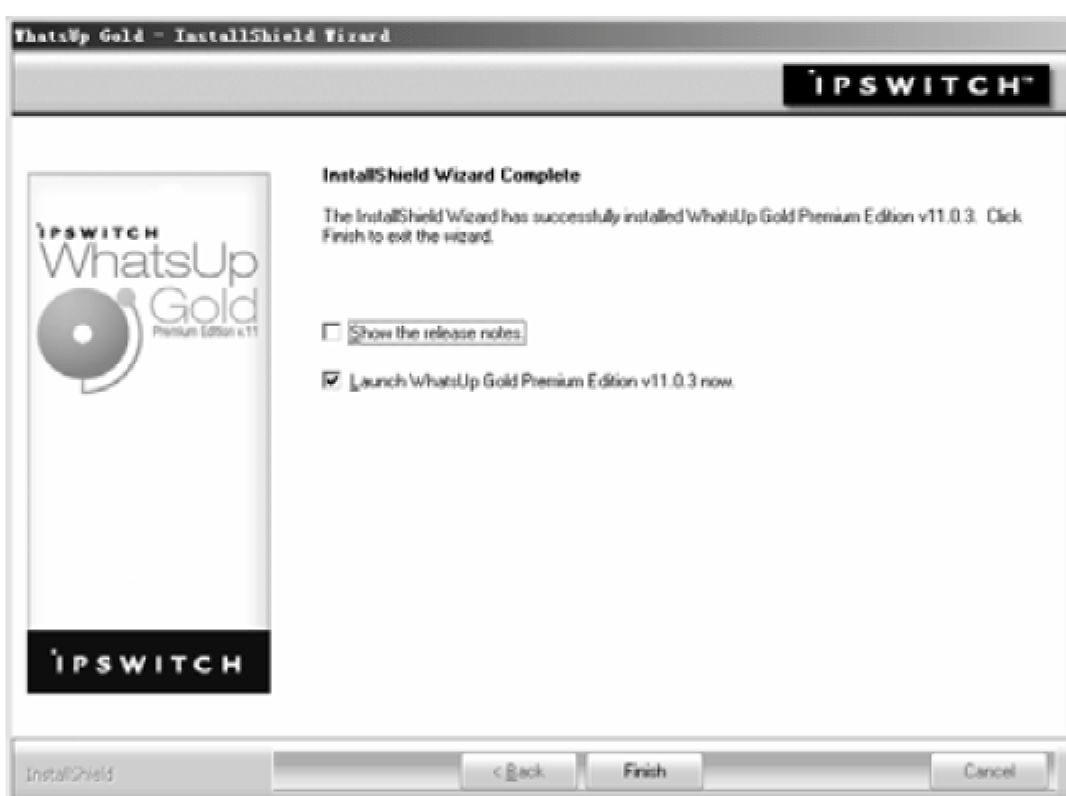


图 17-59　WhatsUp Gold 安装完成

09　系统自动弹出软件激活对话框，选中 Activate Later（稍后激活）复选框，单击【下一步】按钮，到这一步系统已经安装成功，如图 17-60 所示。

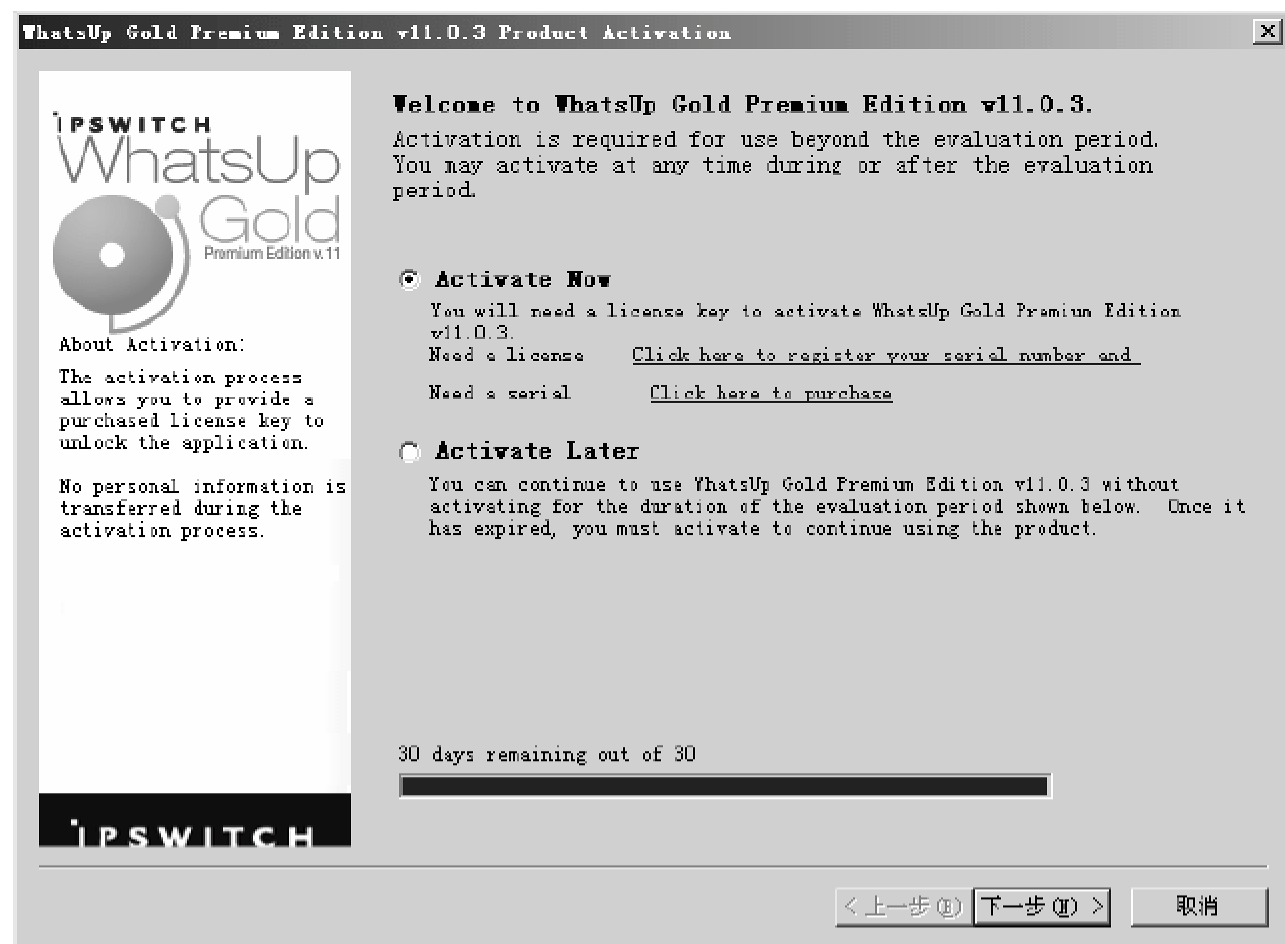


图 17-60　软件激活对话框

17.3.2　实现网络环境监控

使用 WhatsUp Gold 软件监视网络环境，首先要进行网络扫描，获得网络拓扑、设备配置及性能等信息，使用 WhatsUp Gold 软件获取网络拓扑的操作方法如下。

1. 第一次网络扫描

首次运行 WhatsUp Gold 软件，会弹出初次网络扫描的配置向导，使用向导可以轻松地获得第一手网络资料，具体操作步骤如下。

01 启动 WhatsUp Gold 软件，弹出 Setting up the application for the first time（第一次安装应用程序）对话框，单击 Next 按钮，如图 17-61 所示。

02 弹出 Device Discovery Methods（设备发现方法）对话框，选中 IP range scan（扫描 IP 组）单选按钮，单击 Next 按钮，如图 17-62 所示。

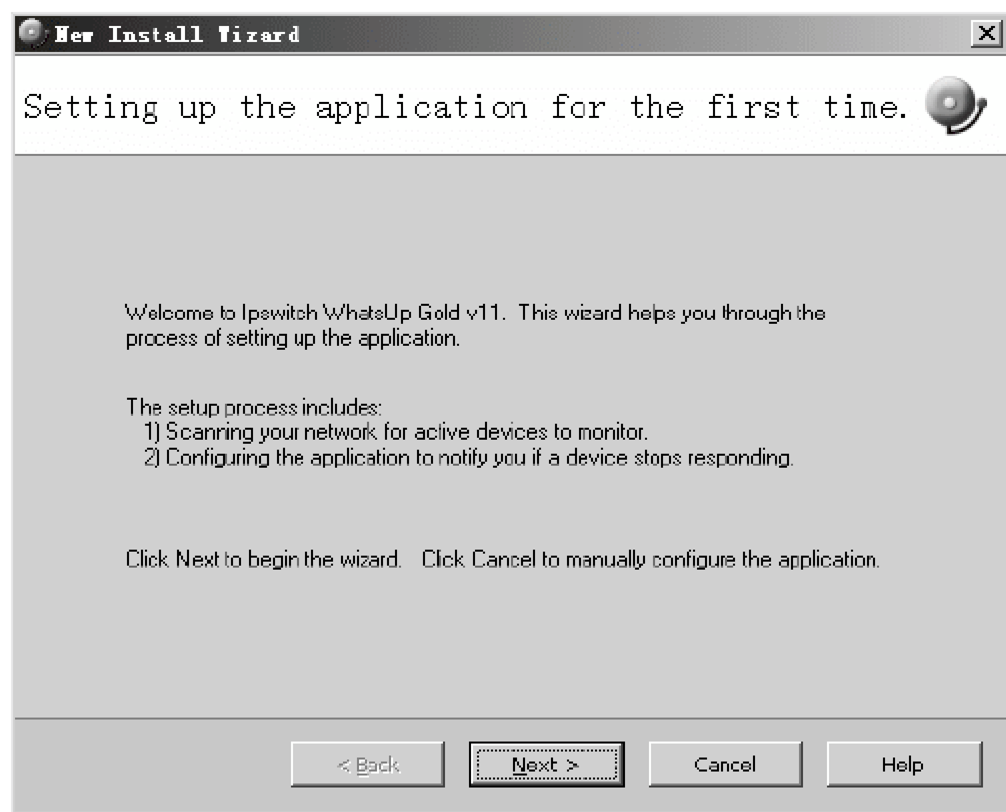


图 17-61　第一次安装程序提示

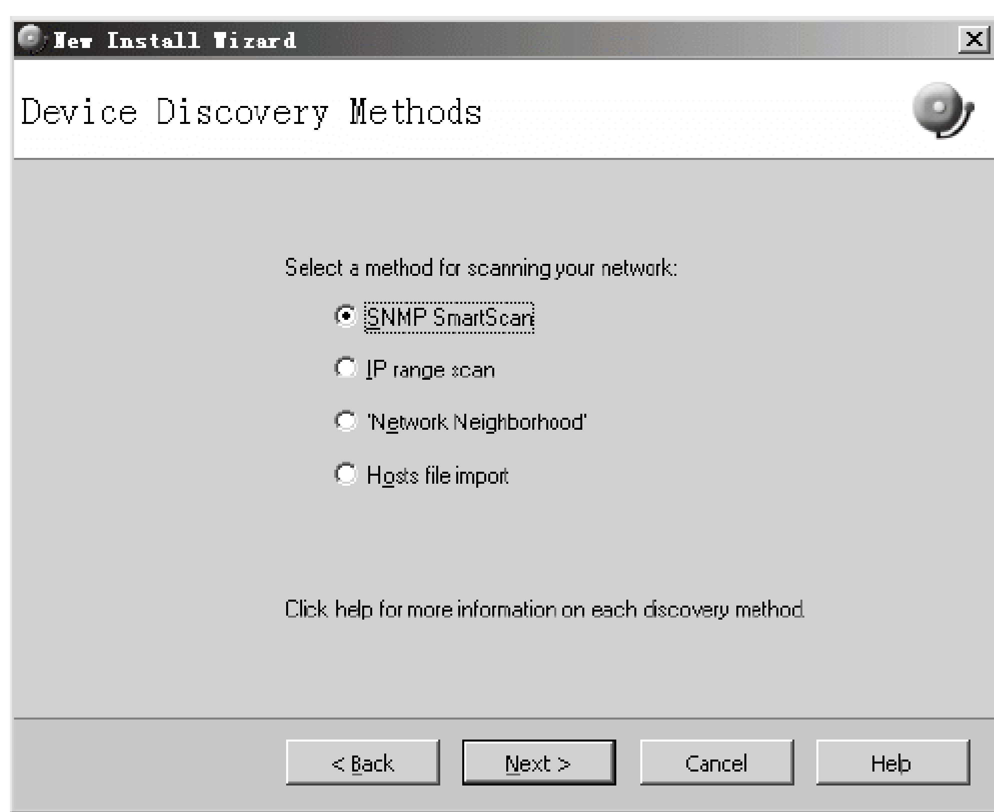


图 17-62　选择扫描设备方法

该对话框中各个参数的含义如下。

- SNMP SmartScan（SNMP 精确扫描）：使用 SNMP 网络管理协议扫描，以团体名为扫描依据。
- IP range scan（IP 组扫描）：针对指定 IP 地址范围进行扫描。
- ‘Network Neighborhood’（网络邻居）：扫描网络邻居。
- Hosts file import（主机文件导入）：依照 Hosts 文件列表进行扫描。

03 弹出 IP Range to Scan（使用 IP 组扫描）对话框，在 Start address（起始地址）文本框中输入起始扫描地址，在 End address（结束地址）文本框中输入终止扫描地址，单击 Next 按钮，如图 17-63 所示。

04 弹出 SNMP Communities（SNMP 团体）对话框，在 SNMP read communities（SNMP 可读团体）文本框中输入 SNMP 团体名，本实例采用默认配置 public，单击 Next 按钮，如图 17-64 所示。

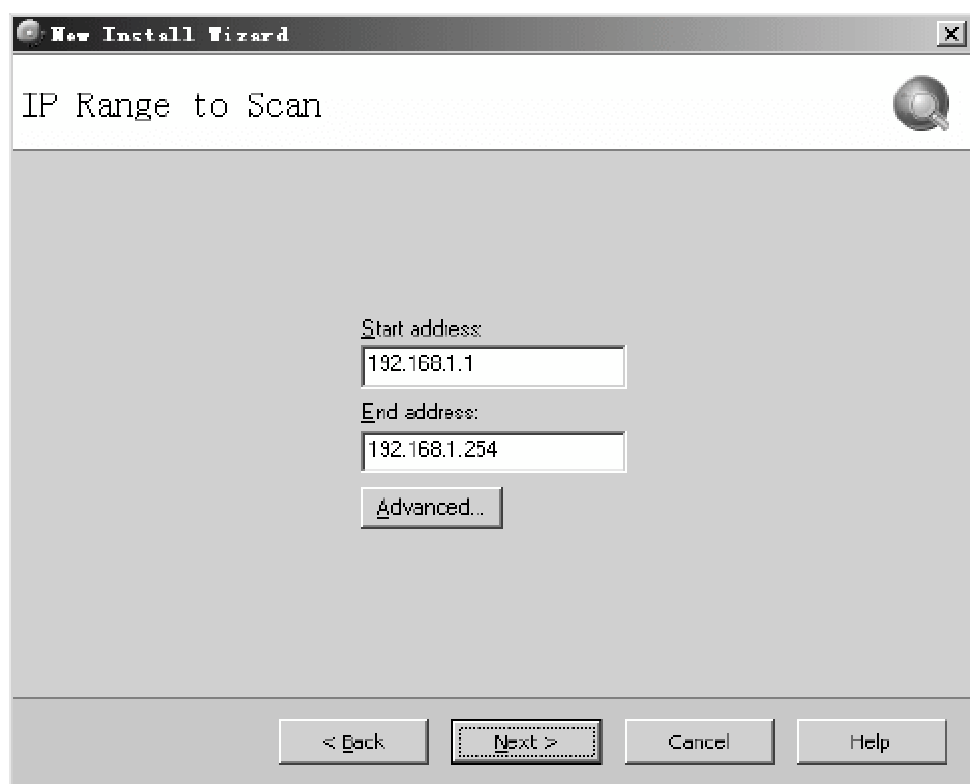


图 17-63 IP Range to Scan 对话框

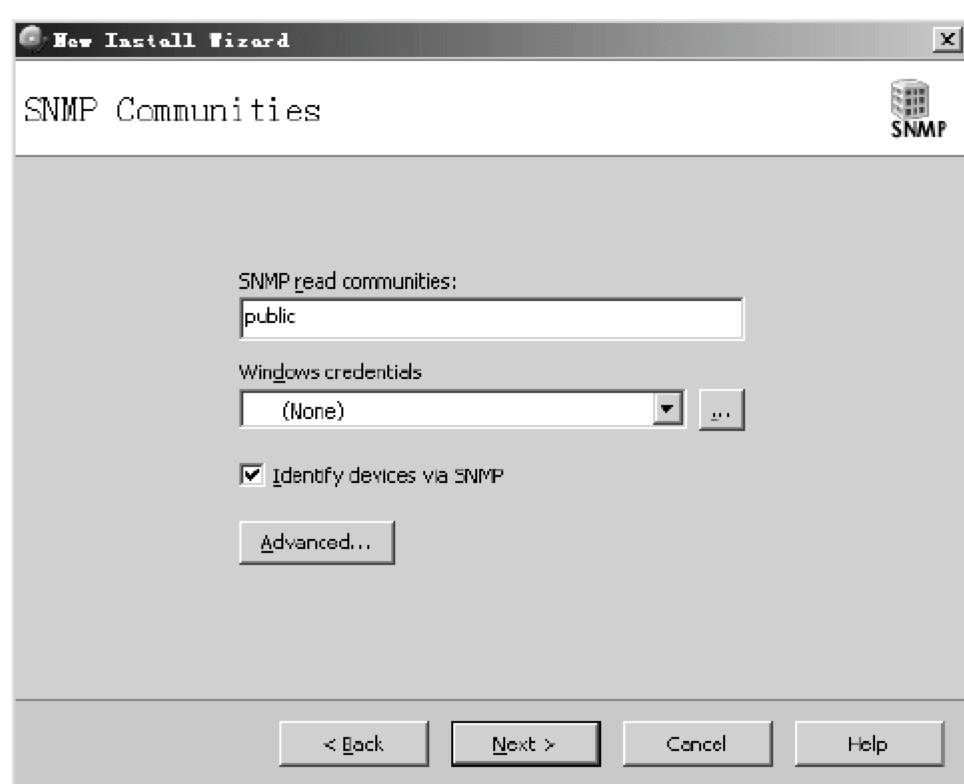


图 17-64 SNMP Communities 对话框

05 弹出 Active/Performance Monitors to Scan（活动/性能显示扫描）对话框，设置扫描活动协议状态及设备性能信息，单击 Next 按钮，如图 17-65 所示。

06 系统自动开始扫描网络，并显示扫描进度，如图 17-66 所示。

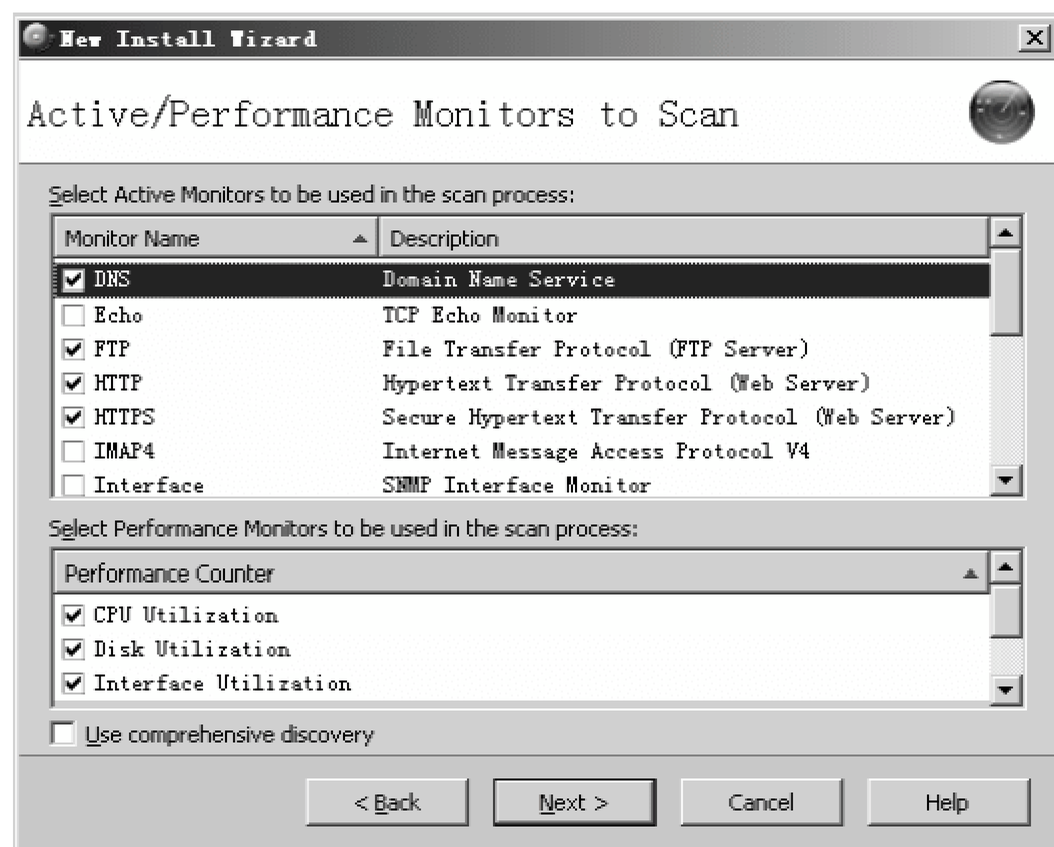


图 17-65 Active/Performance Monitors to Scan 对话框

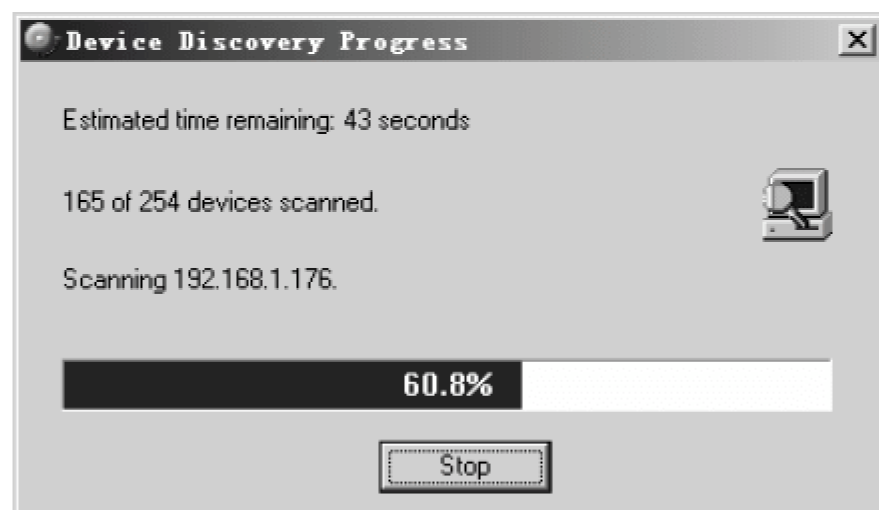


图 17-66 自动扫描网络

07 扫描结束后弹出 Devices to Monitor（设备显示列表）对话框，显示扫描结果，选择需显示设备左侧的复选框，单击 Next 按钮，如图 17-67 所示。

08 弹出 Action Policy Selection（选择动作策略）对话框，选中 Assist in creating a new action policy(设置新动作策略)单选按钮，单击 Nex 按钮，如图 17-68 所示。

09 弹出 Action Strategies（动作策略）对话框，共有三部分内容的设置，分别是：【If a device has been unresponsive for 5 minutes，notify me by】（如果一个设备丢失 5 分钟如何提醒我）、【If a device has been unresponsive for 20 minutes，notify me by】（如果一个设备丢失 20 分钟如何提醒我）、【When a device starts responding again，notify me by】（当一个设备重新连接时如何提醒我）。可以通过 E-mail 邮件、提示音、message window 三种方式进行提醒，这里三项均选择 E-mail 邮件和提示音方式，单击 Next 按钮，如图 17-69 所示。

10 弹出 Internet E-mail Address（邮箱地址设置）对话框，在 E-mail address（邮件地址）文本框中输入有效的邮箱地址，在 Outgoing mail（SMTP）server（向外发送邮件 SMTP 服务器）文

本框中输入 SMTP 服务器地址，单击 Next 按钮，如图 17-70 所示。

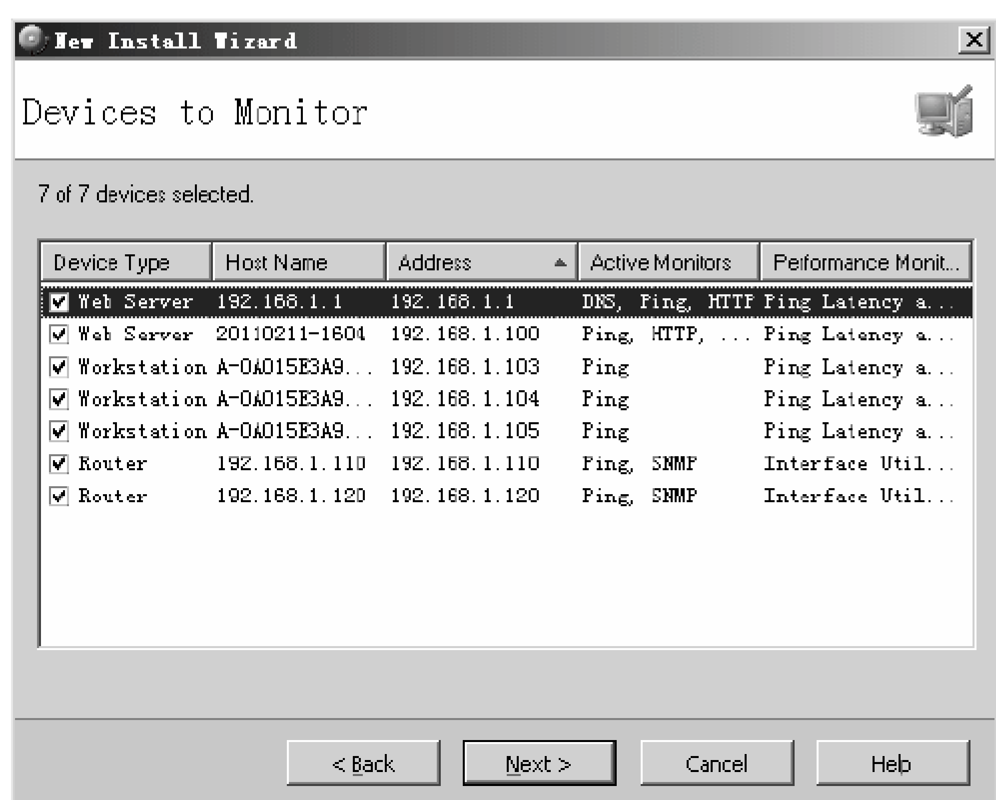


图 17-67　Devices to Monitor

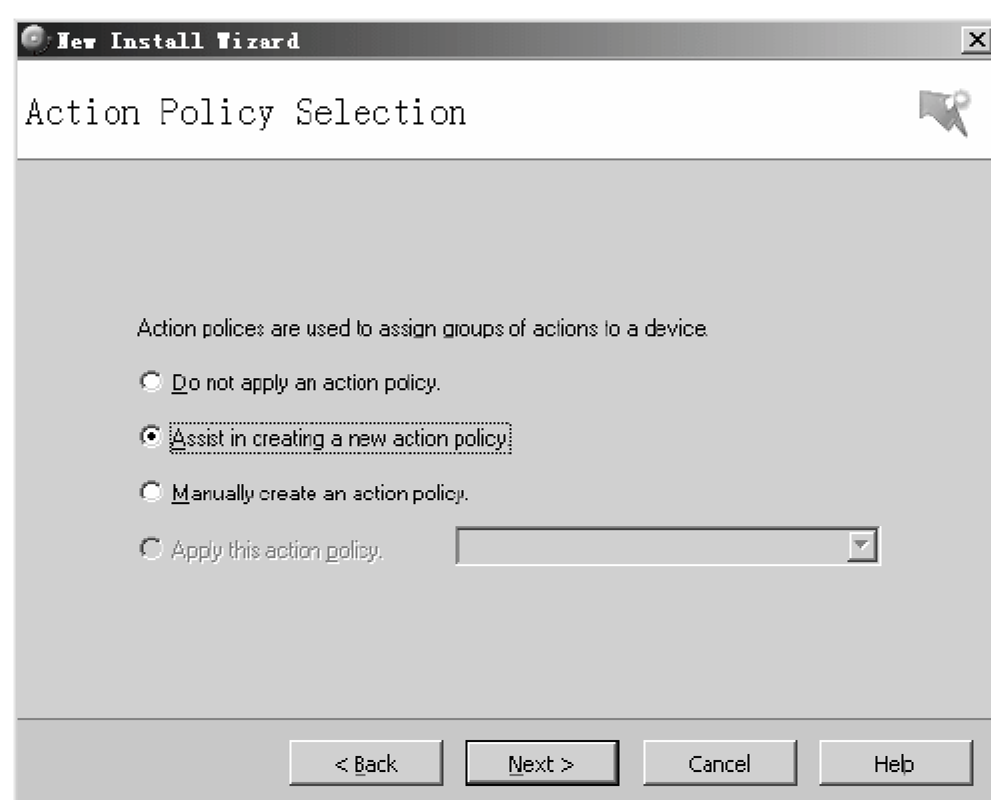


图 17-68　Action Policy Selection

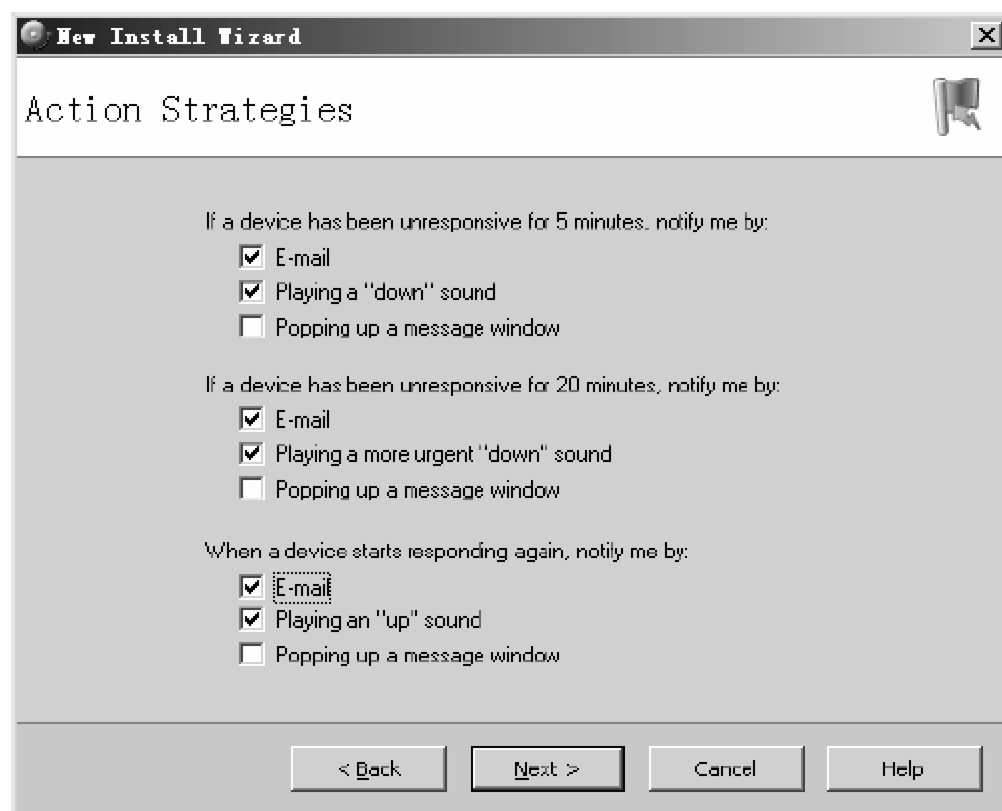


图 17-69　Action Strategies 对话框

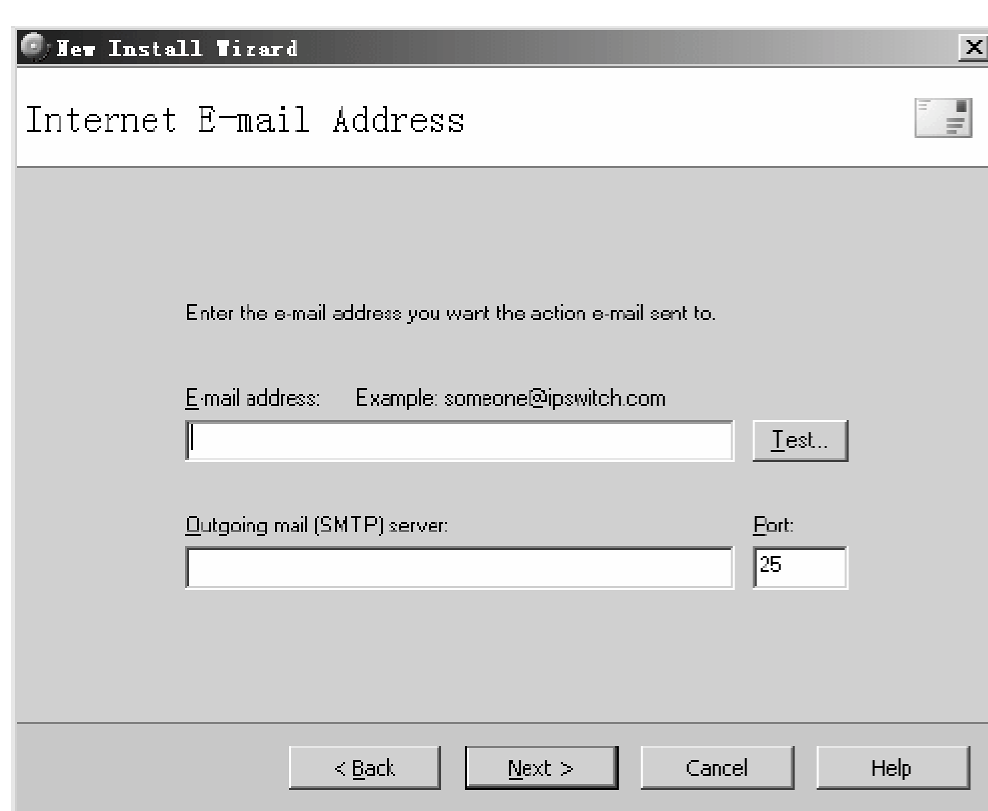


图 17-70　Internet E-mail Address 对话框

11 弹出 Action Policy Summary（动作策略命名）对话框，在 Policy name（策略名）文本框中输入策略名，本实例采用默认配置，单击 Next 按钮，如图 17-71 所示。

12 弹出 Finish 对话框，在其中显示出已配置的策略，单击 Finish 按钮，如图 17-72 所示。

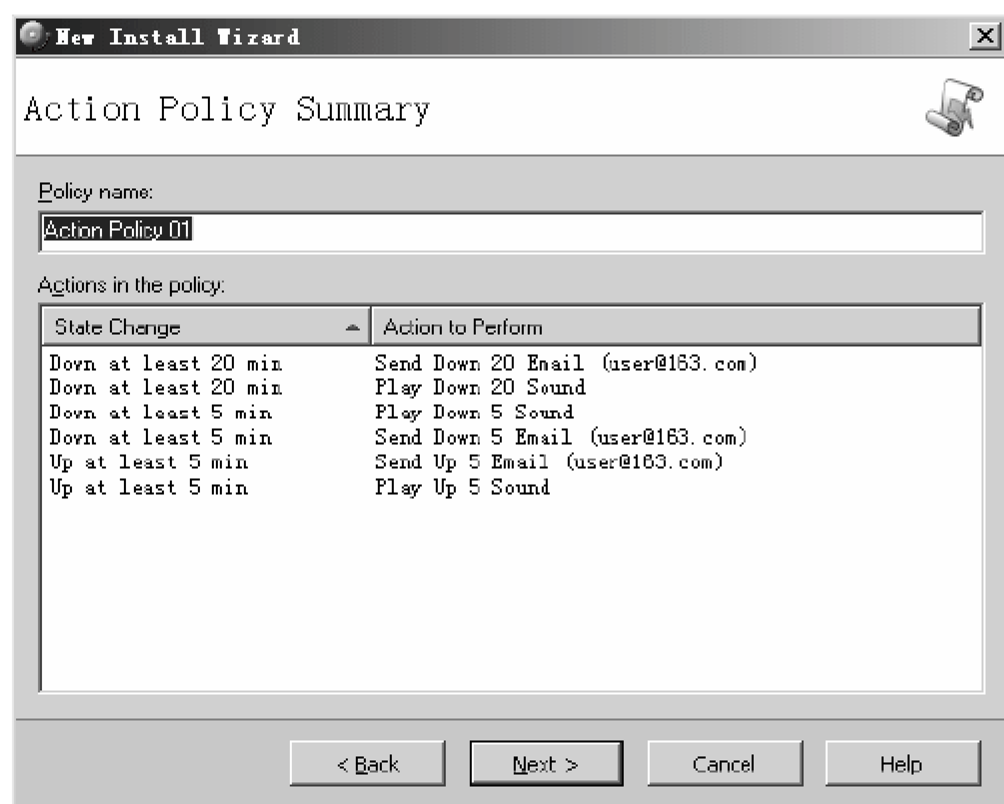


图 17-71　Action Policy Summary 对话框

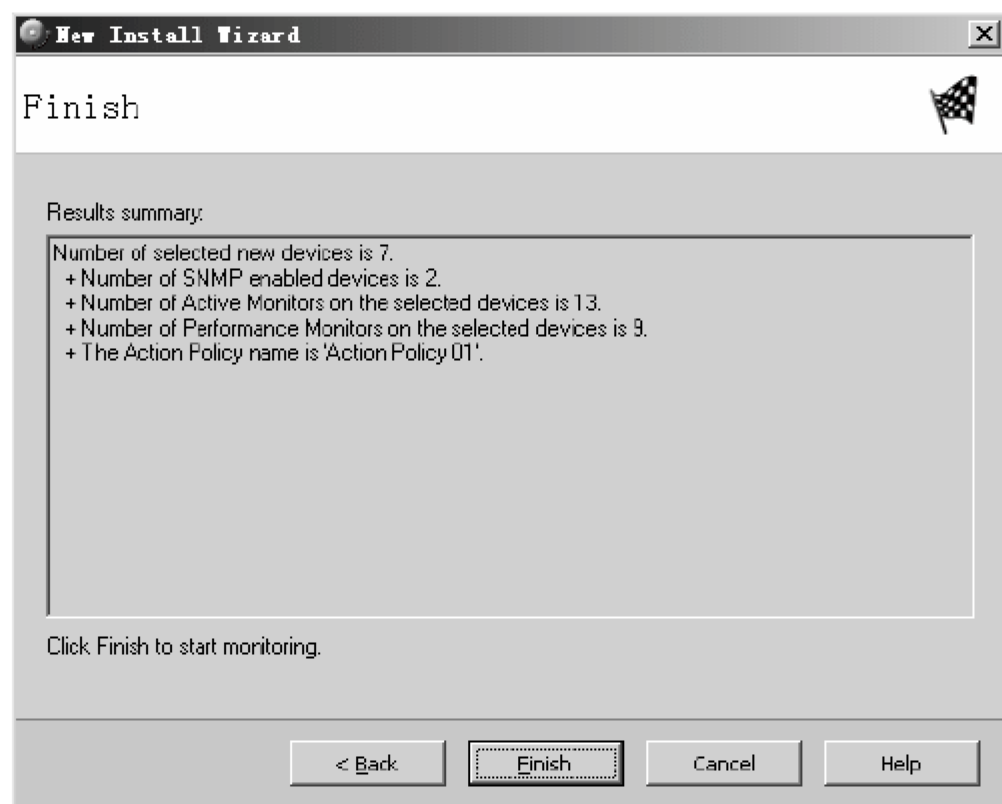


图 17-72　Finish 对话框

13 进入 WhatsUp Gold 程序主界面，窗口右侧显示了扫描结果，显示信息包括设备名、地址、设备类型等，如图 17-73 所示。

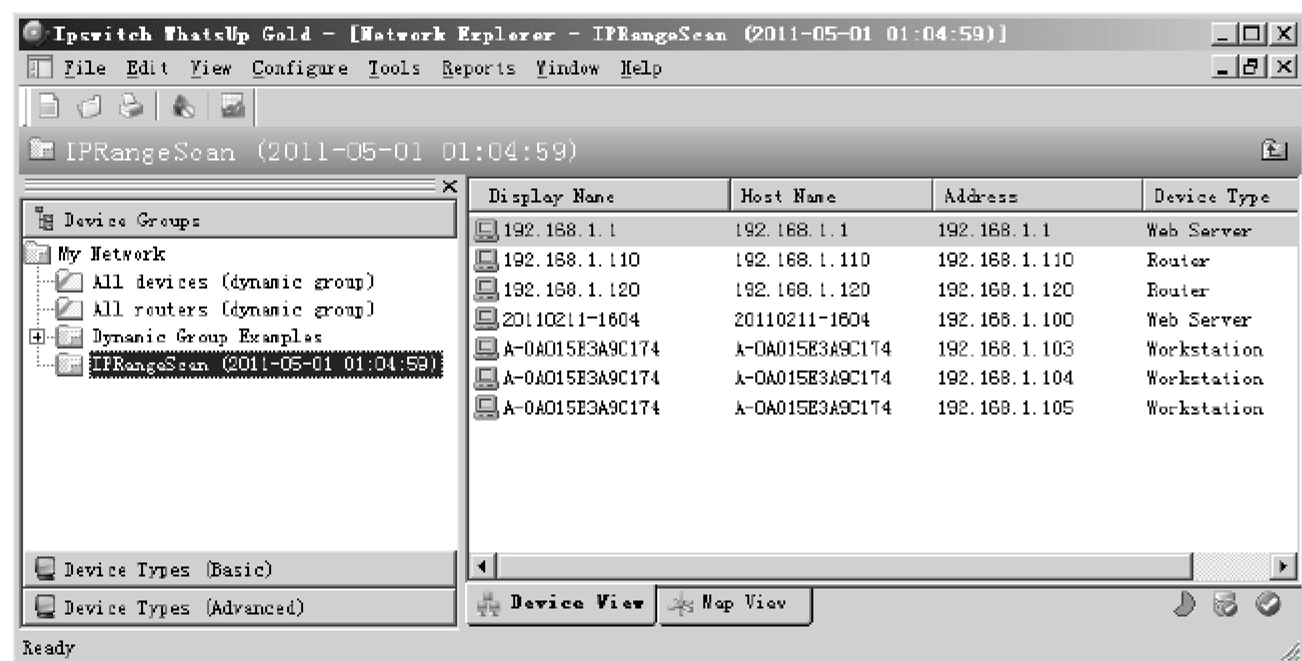


图 17-73　WhatsUp Gold 程序主界面

14 打开 Map View（地图视图）选项卡，使用视图形式查看网络设备，如图 17-74 所示。

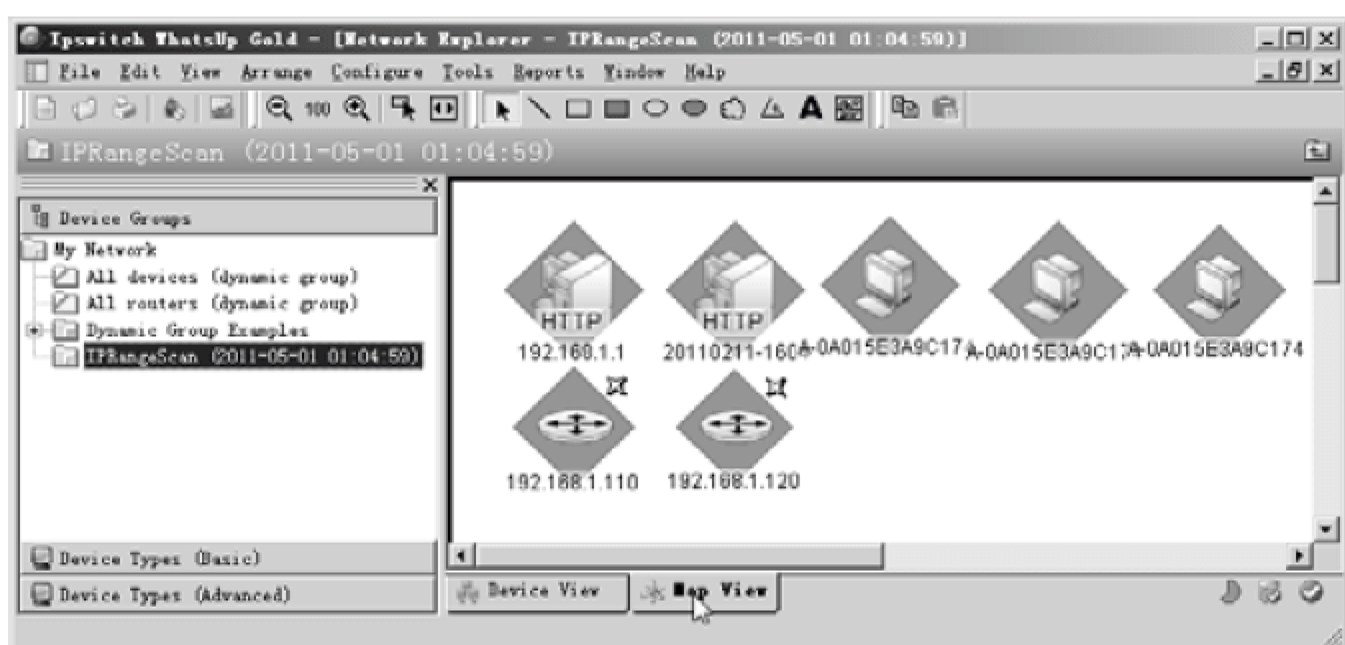


图 17-74　选择 Map View 模式

2. 拓展网络拓扑

第一次扫描往往不能获取网络内所有设备的信息，需要管理员手工添加未扫描到的设备，以完善网络拓扑结构。

添加新设备的具体操作步骤如下。

01 在 WhatsUp Gold 主界面左侧选择 Device Types（Basic）（基本设备类型）选项列表，列表中显示了很多可添加的设备类型，如图 17-75 所示。

02 选择需要添加的设备类型，如 Router（路由器），将其拖曳到右侧视图界面，如图 17-76 所示。

03 弹出 Add New Device 对话框，在 IP address or host name of the new device（新设备 IP 地址或主机名）文本框中输入要添加设备的 IP 地址或主机名，本实例采用“172.16.1.2”主机为例进行讲解，单击 Advanced 按钮，如图 17-77 所示。

04 在弹出的对话框中选择需要获得目标设备的哪些信息，单击 OK 按钮，如图 17-78 所示。

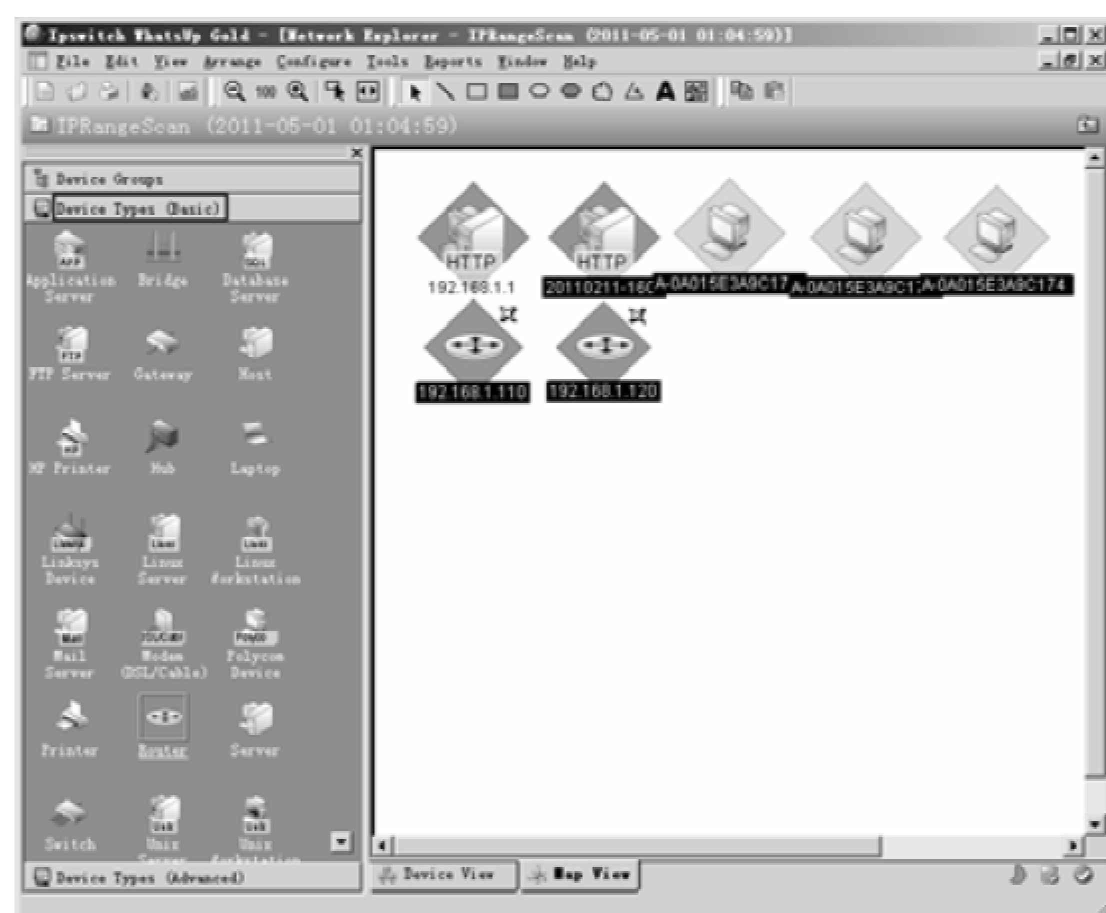


图 17-75 Device Types（Basic）选项列表

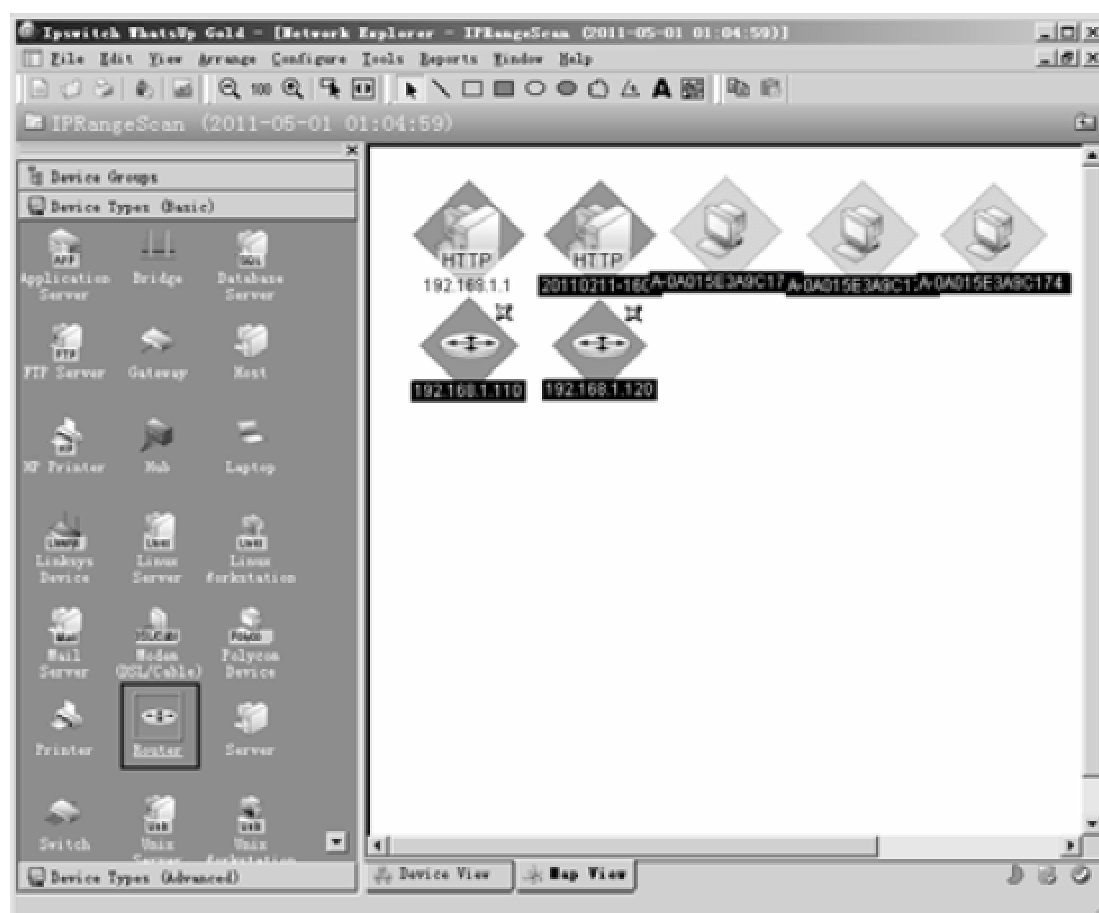


图 17-76 添加路由器设备



图 17-77 Add New Device 对话框

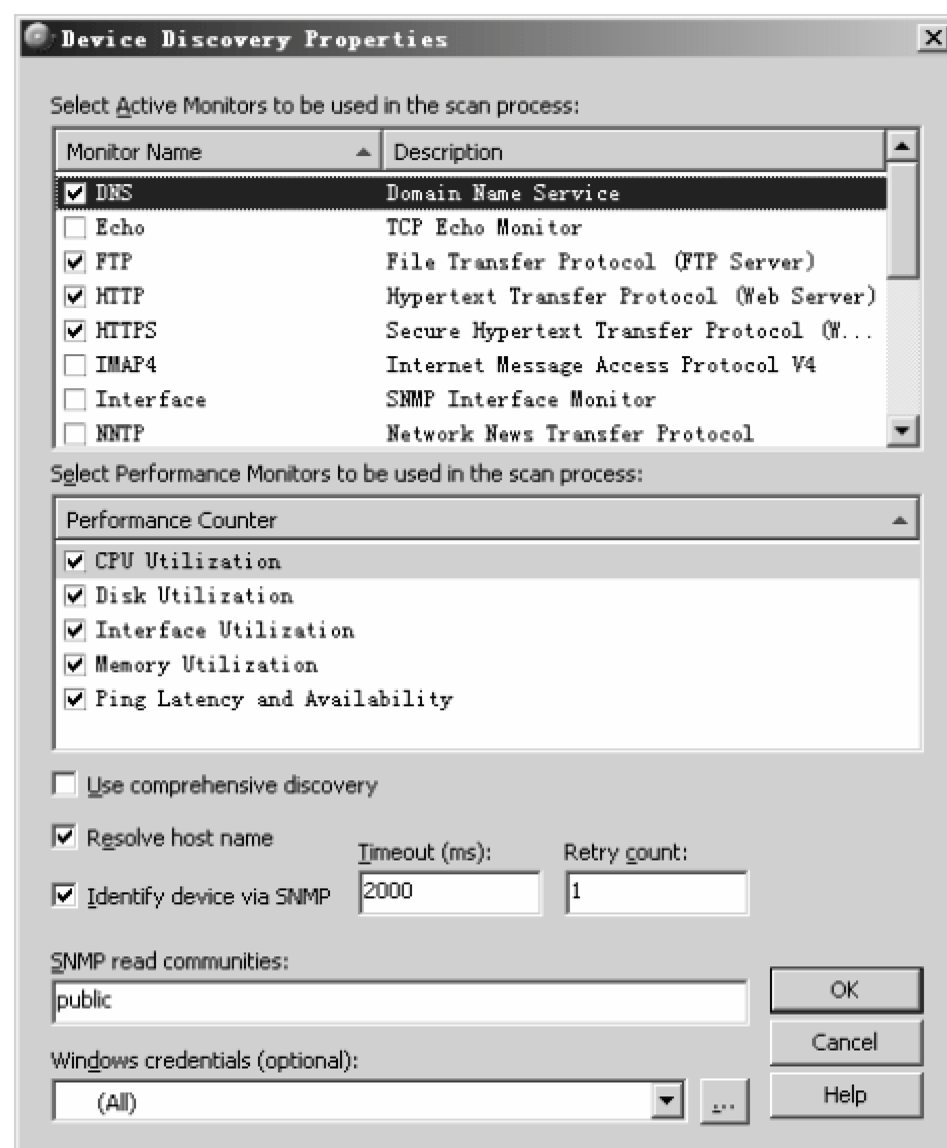


图 17-78 选择需要显示的设备信息

05 返回 Add New Device 对话框，单击 OK 按钮，如图 17-79 所示。

06 系统自动扫描主机信息，并显示扫描进度，如图 17-80 所示。



图 17-79 Add New Device 对话框

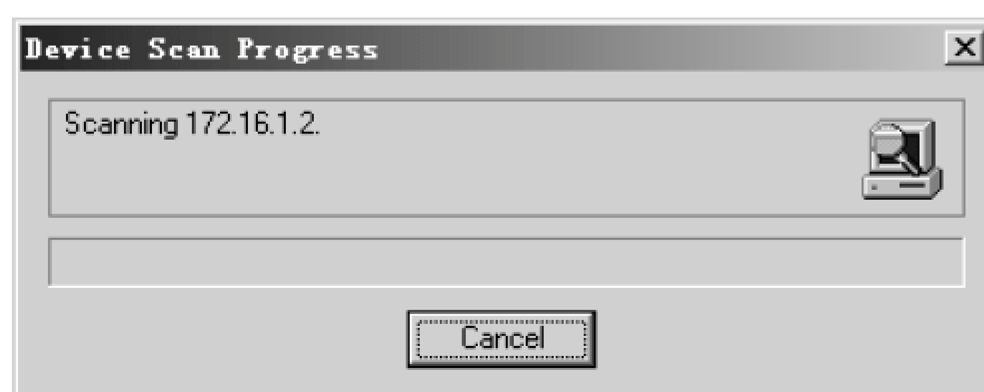


图 17-80 系统自动扫描主机信息

07 扫描结束，自动弹出设备 172.16.1.2 的基本信息配置界面，本实例采用默认配置，单击 OK 按钮，如图 17-81 所示。

08 设备“172.16.1.2”添加成功，设备图标显示在右侧视图窗口，绿色表示设备可连通，如图 17-82 所示。

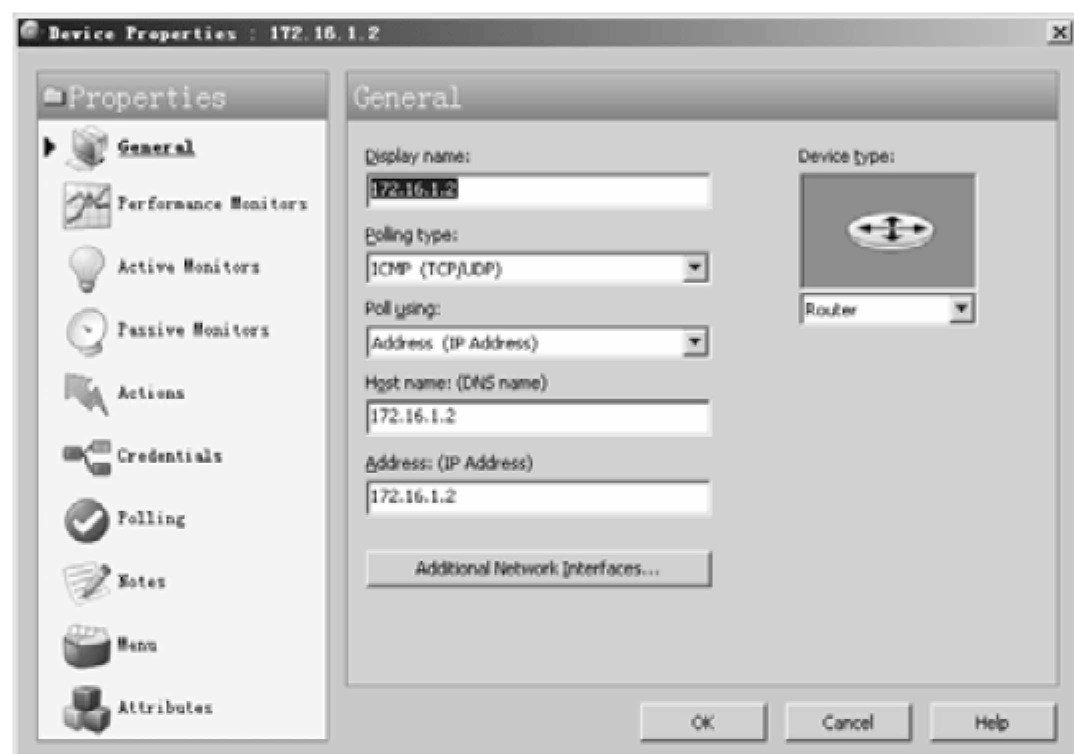


图 17-81　设备信息配置界面

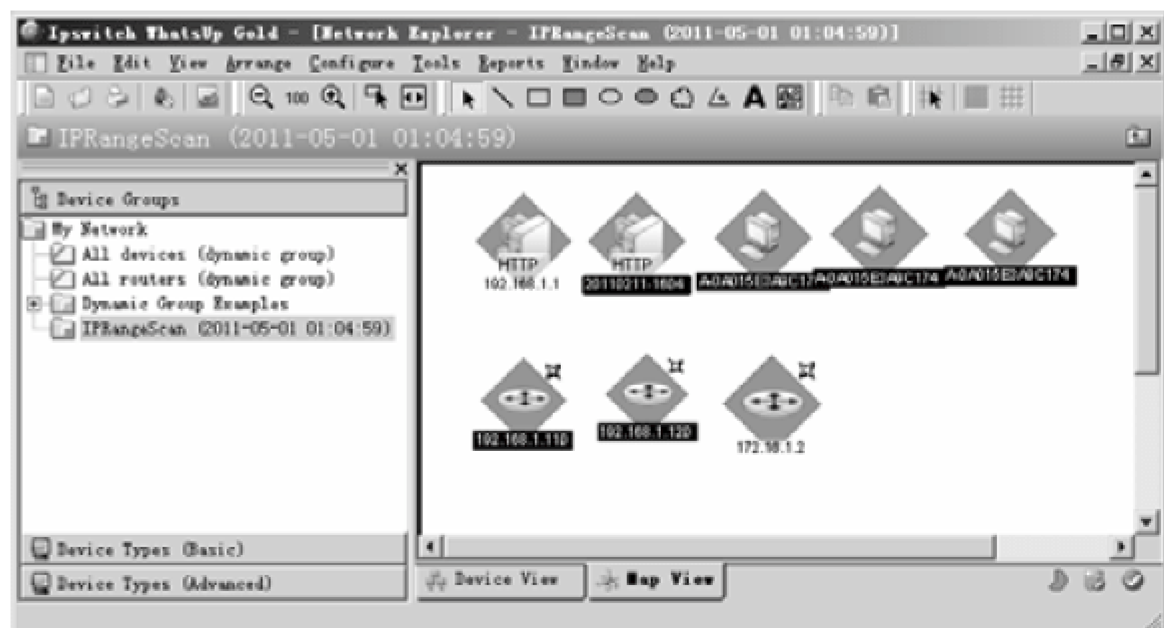


图 17-82　设备添加成功

3. 调整设备连接关系，绘制网络拓扑图

设备添加成功后，只可以看到设备图标，但是无法看到所有设备的连接关系，不能直观地查看网络拓扑图，连接关系需要手工添加。

添加连接关系，绘制网络拓扑图的具体操作步骤如下。

01 右击图 17-83 中某一网络设备，在弹出的快捷菜单中选择 Link ➢ Link to 命令。

02 弹出 Select a Monitor to Link（挑选一种方式连接）对话框，选择适当的测试连通方式，本实例采用 ping 方式，单击 OK 按钮，如图 17-84 所示。

03 鼠标指针显示带有“+”号的短线，单击要连接的设备，如图 17-85 所示。

04 选择的两个设备会通过 ping 命令测试连接状态，链接关系建立成功后如图 17-86 所示。

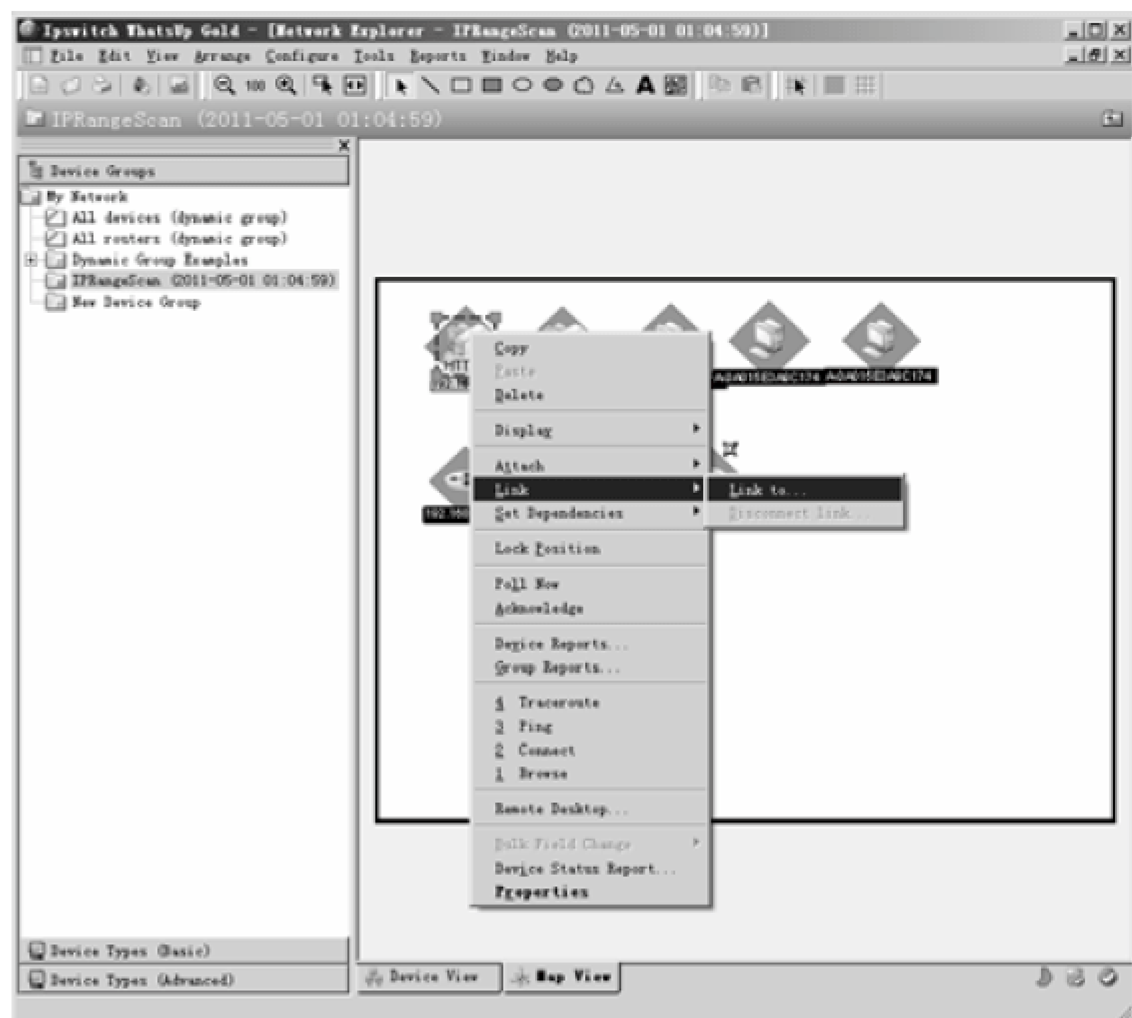


图 17-83　进行设备连接

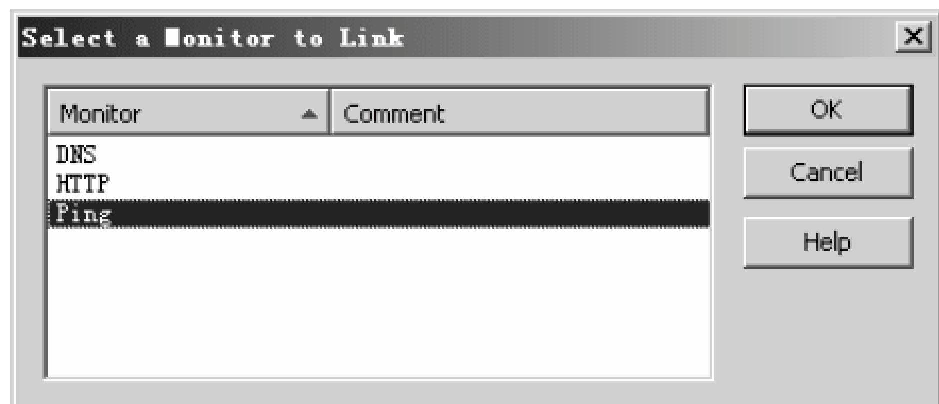


图 17-84　Select a Monitor to Link 对话框

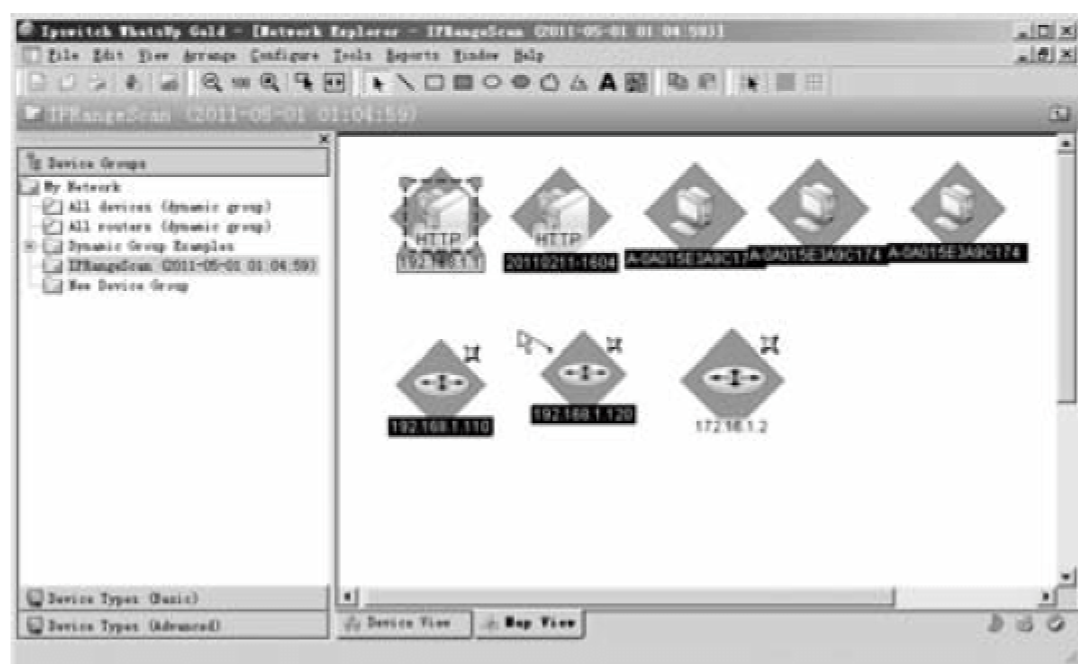


图 17-85　选择要连接的设备

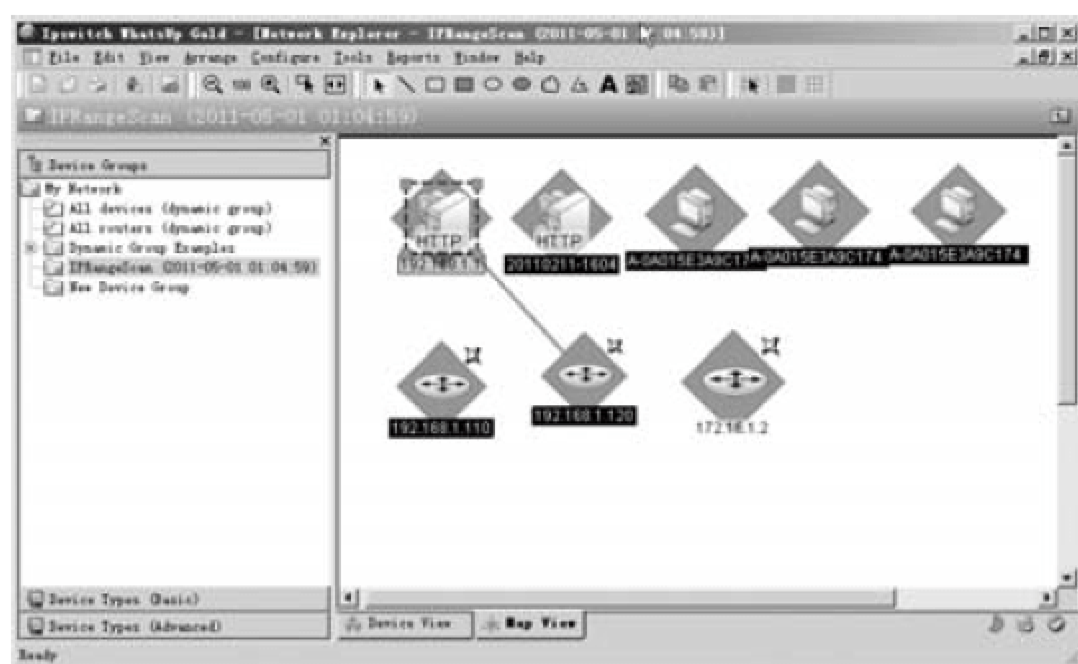


图 17-86　设备连接成功

05 根据网络设备连接状况，添加所有设备及连接关系，形成最终的网络拓扑图，如图 17-87 所示。

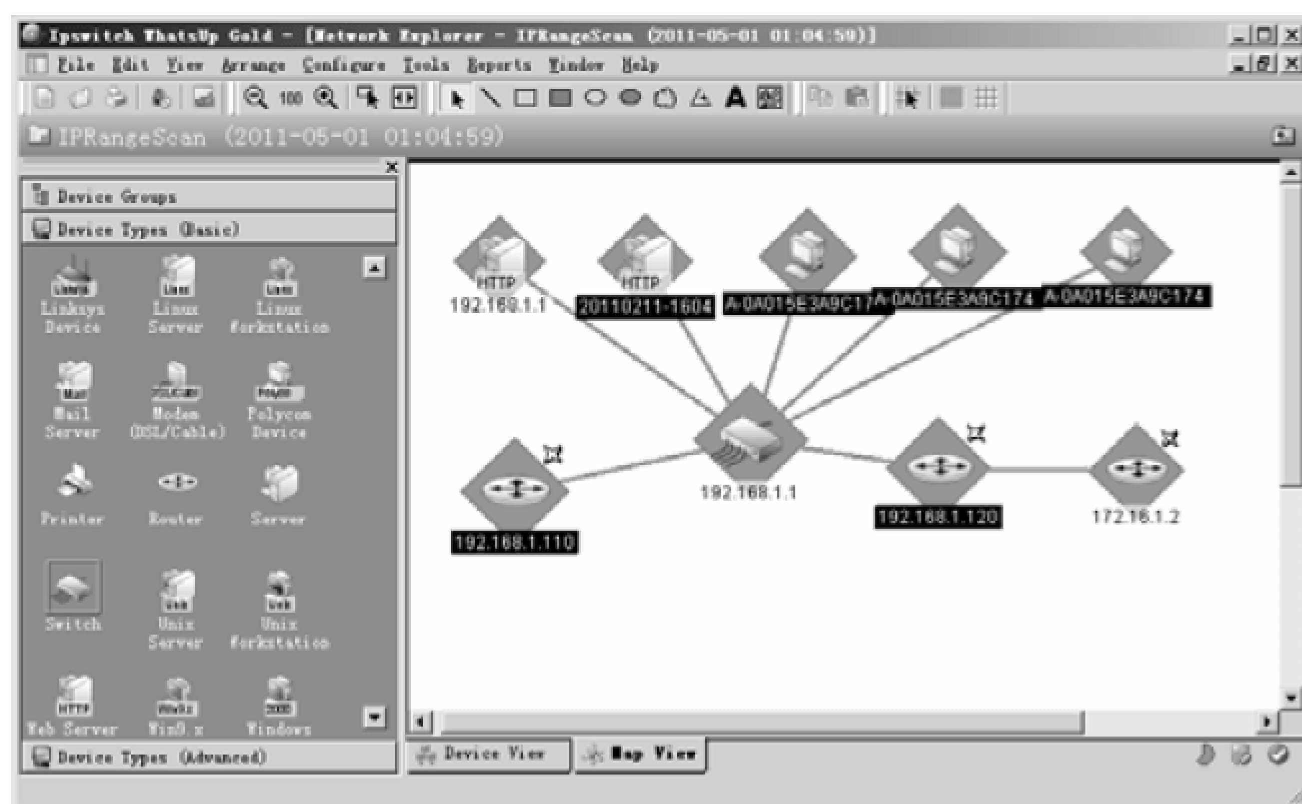


图 17-87　添加所有设备连接

17.3.3　查看网络设备信息

使用 WhatsUp Gold 可以通过网页形式查看设备的信息，具体操作步骤如下。

01 右击需要查看的设备图标，在弹出的快捷菜单中选择 Device Reports（设备报告）命令，如图 17-88 所示。

02 打开 WhatsUp Gold 网页登录页面，在 User Name（用户名）文本框中输入登录用户名，在 Password（密码）文本框中输入登录密码，用户名和密码均默认为 admin，单击 Login 按钮，如图 17-89 所示。

03 进入设备报告查看页面，单击页面内的选项可以查看到各种相关信息，如图 17-90 所示。

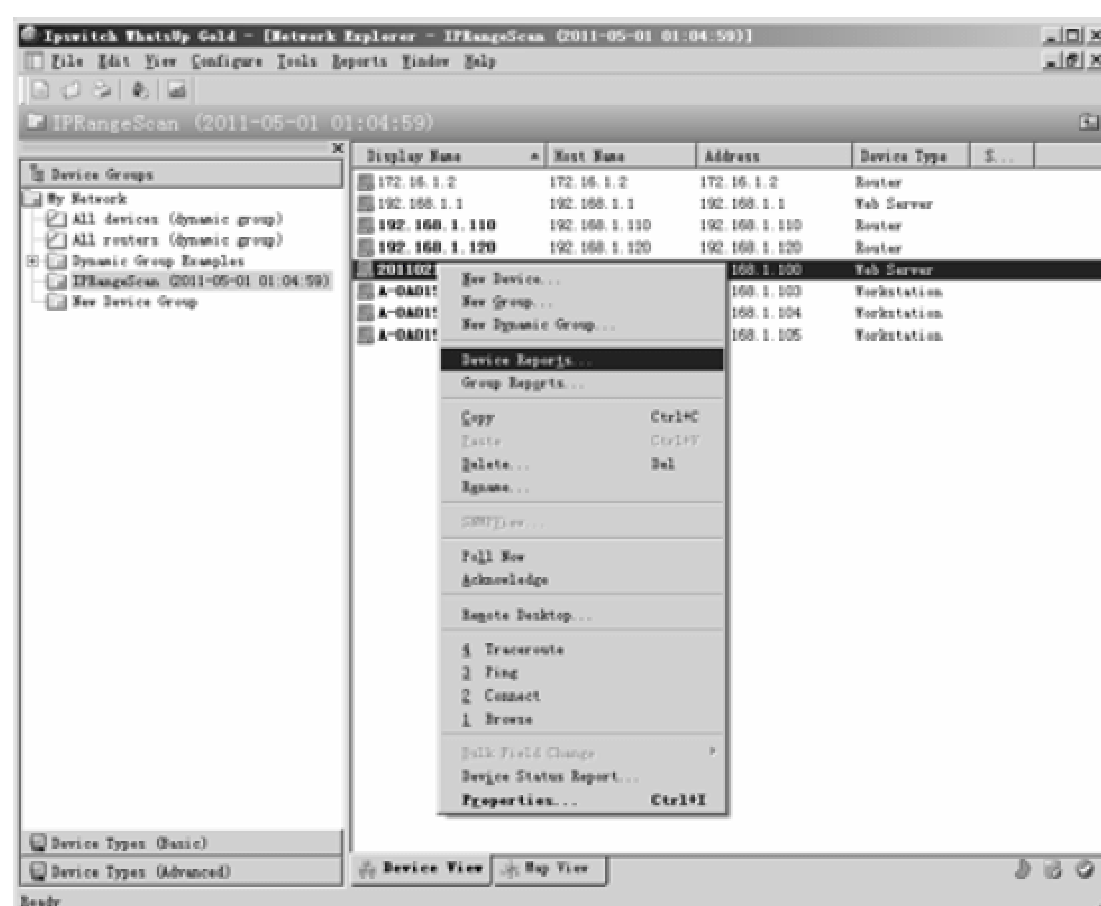


图 17-88　查看设备信息



图 17-89　WhatsUp Gold 网页登录页面

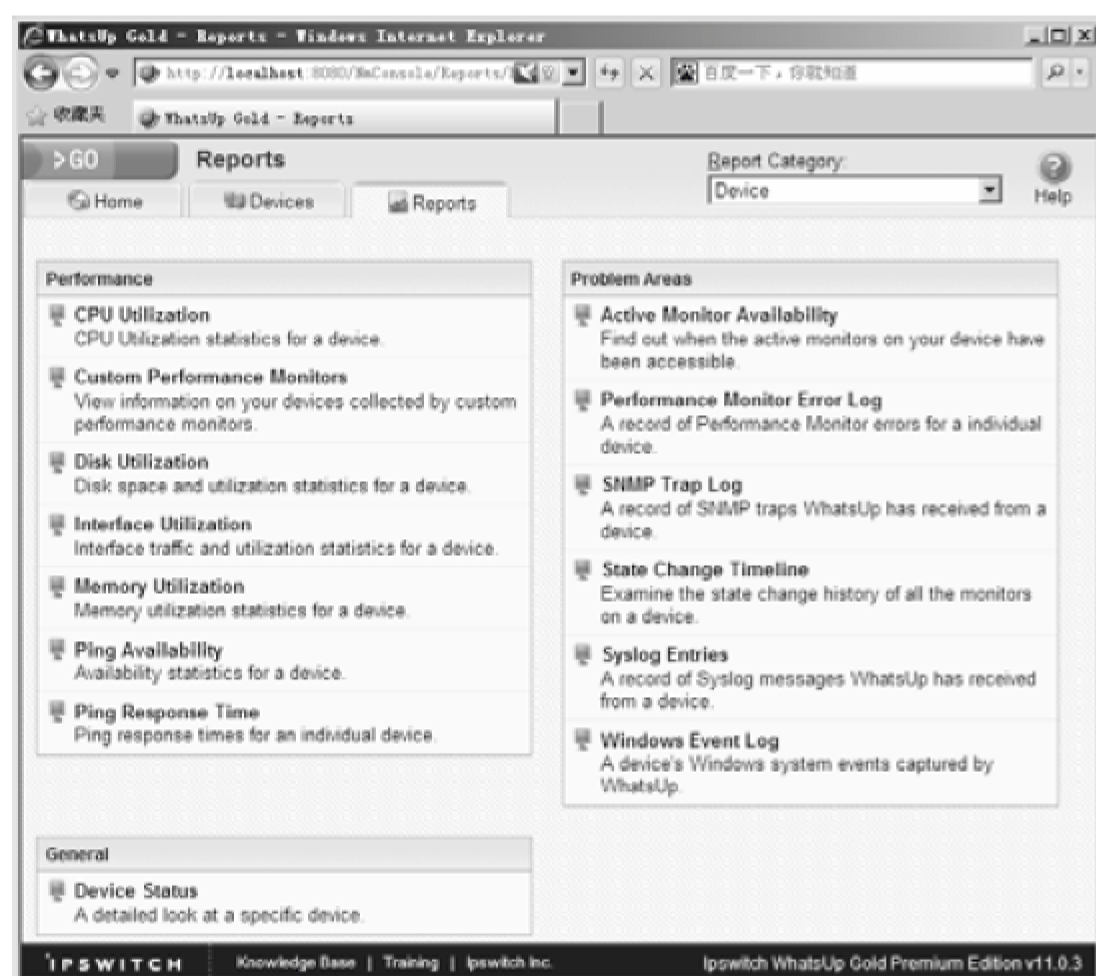


图 17-90　设备报告查看页面

04 打开 Devices 选项卡，在右侧窗口中双击需要查看信息的设备，本实例使用“192.168.1.120”为例进行讲解，如图 17-91 所示。

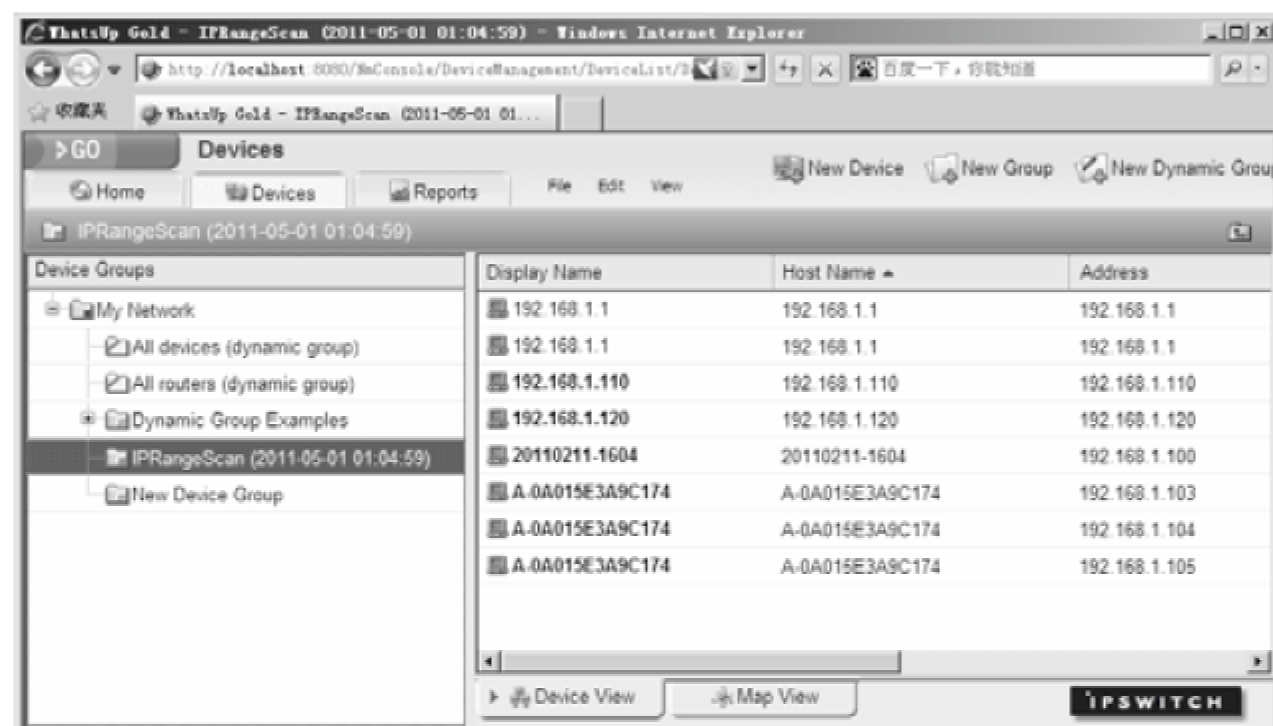


图 17-91 Devices 选项卡

05 进入设备“192.168.1.120”的信息统计界面，通过界面可以获得设备的性能列表、基本信息、日志信息、SNMP 协议信息等，如图 17-92 所示。

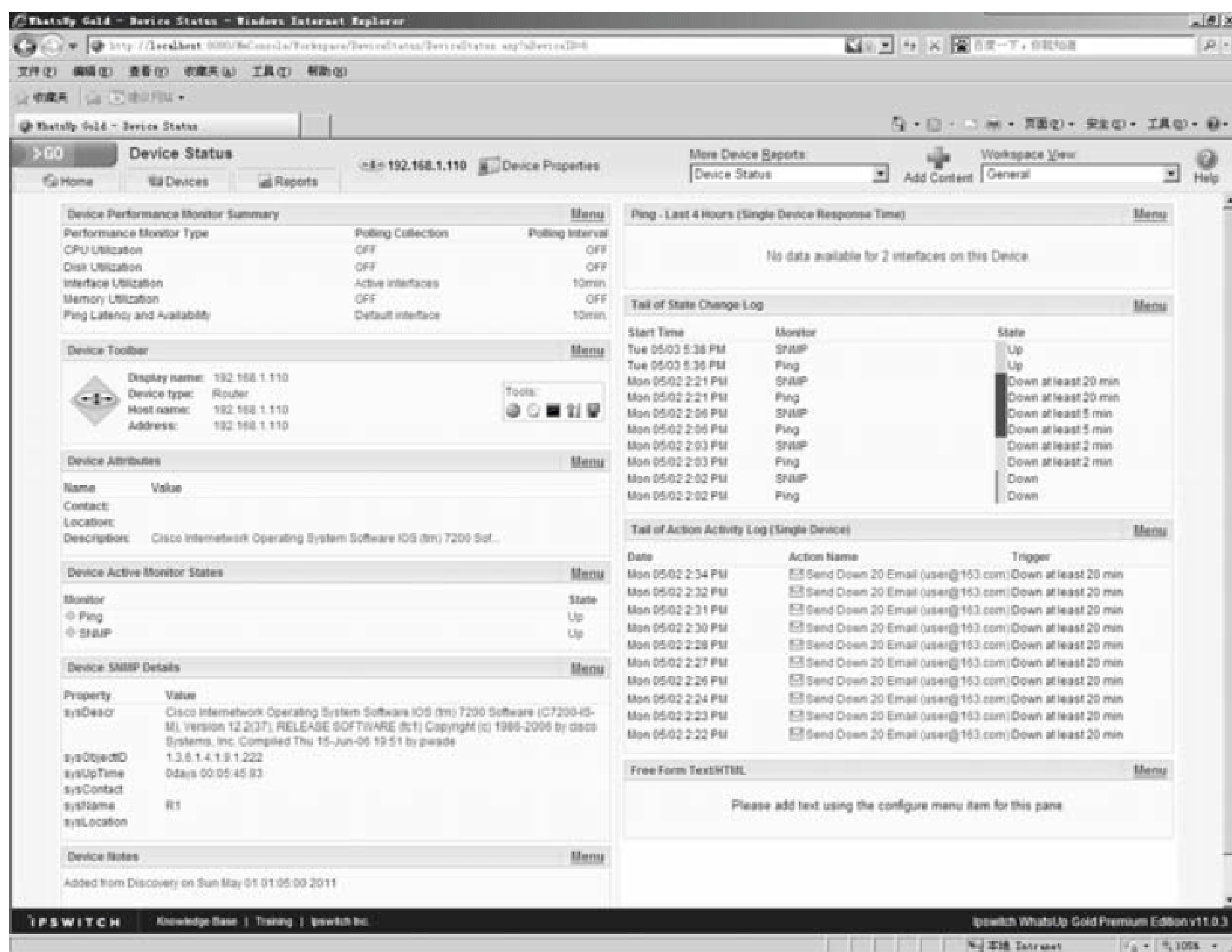


图 17-92 目标设备信息统计界面

17.3.4 网络故障发现与修复

网络运营中会出现很多链接问题，通过 WhatsUp Gold 可以清晰地看出故障问题，具体显示效果如下。

（1）网络设备刚断开时，设备图标形状和颜色变化如图 17-93 所示。

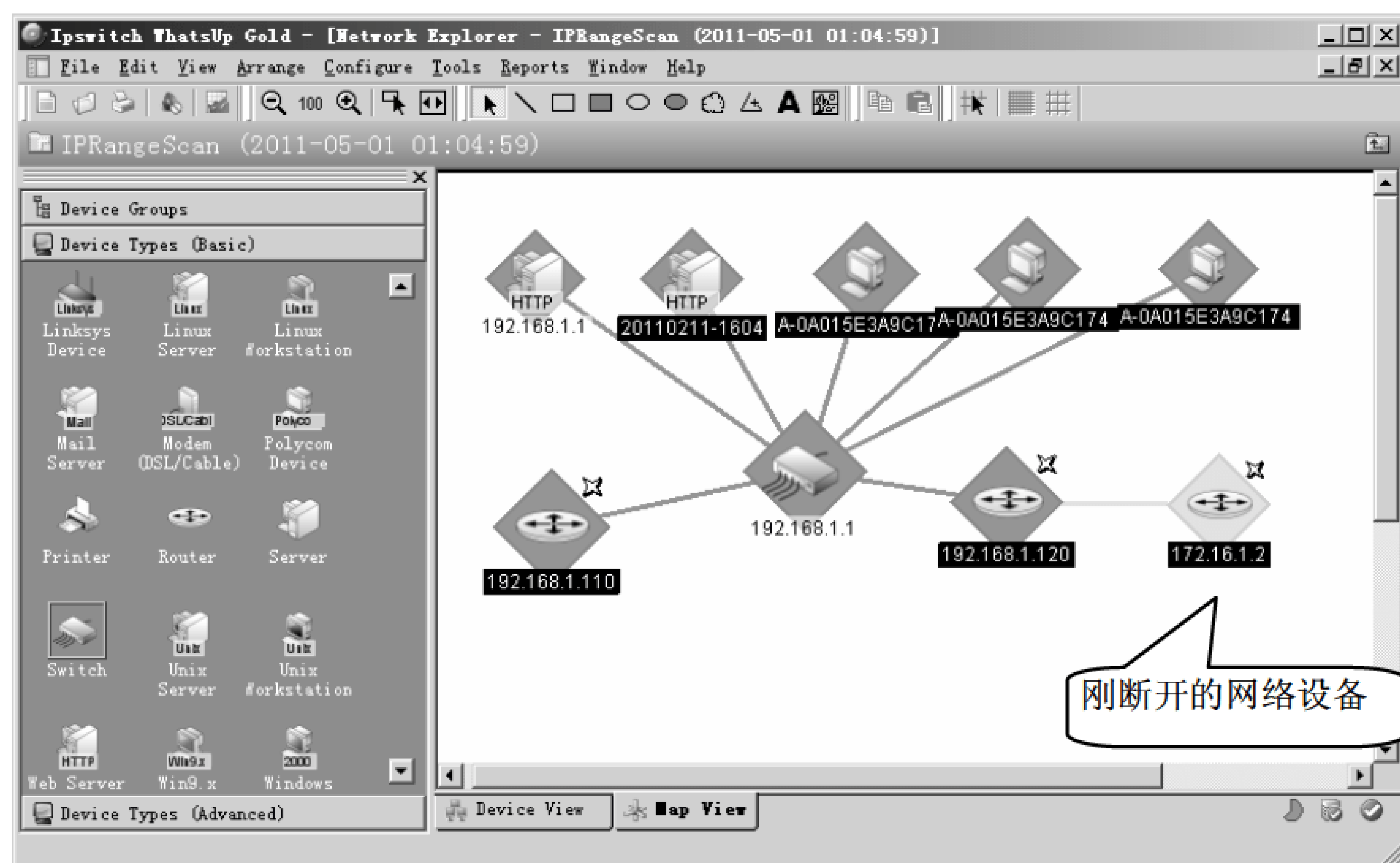


图 17-93　网络设备刚断开

（2）网络设备断开 2 分钟后，设备图标形状和颜色变化如图 17-94 所示。

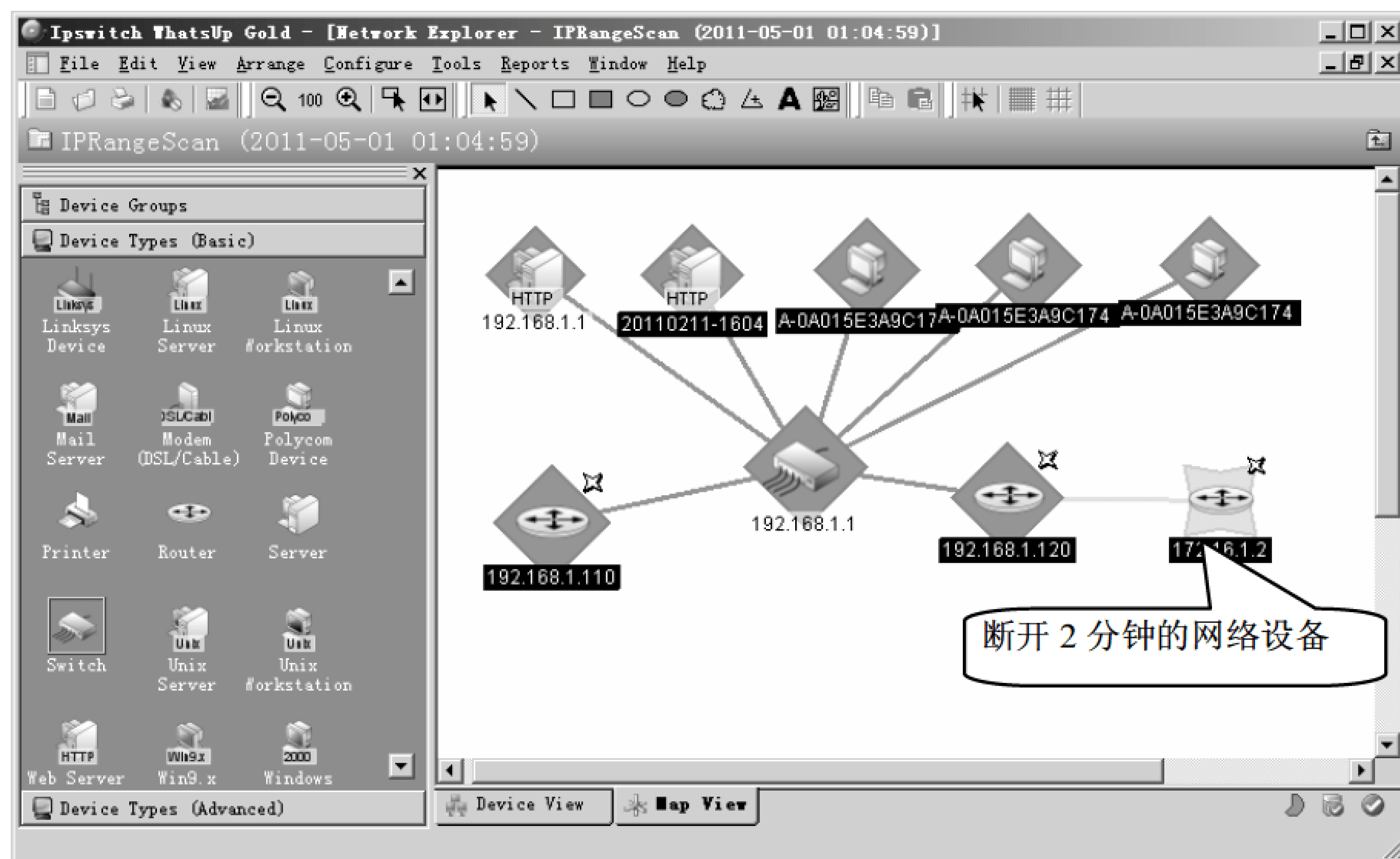


图 17-94　网络设备断开 2 分钟

（3）网络设备断开 5 分钟后，设备图标形状和颜色变化如图 17-95 所示。

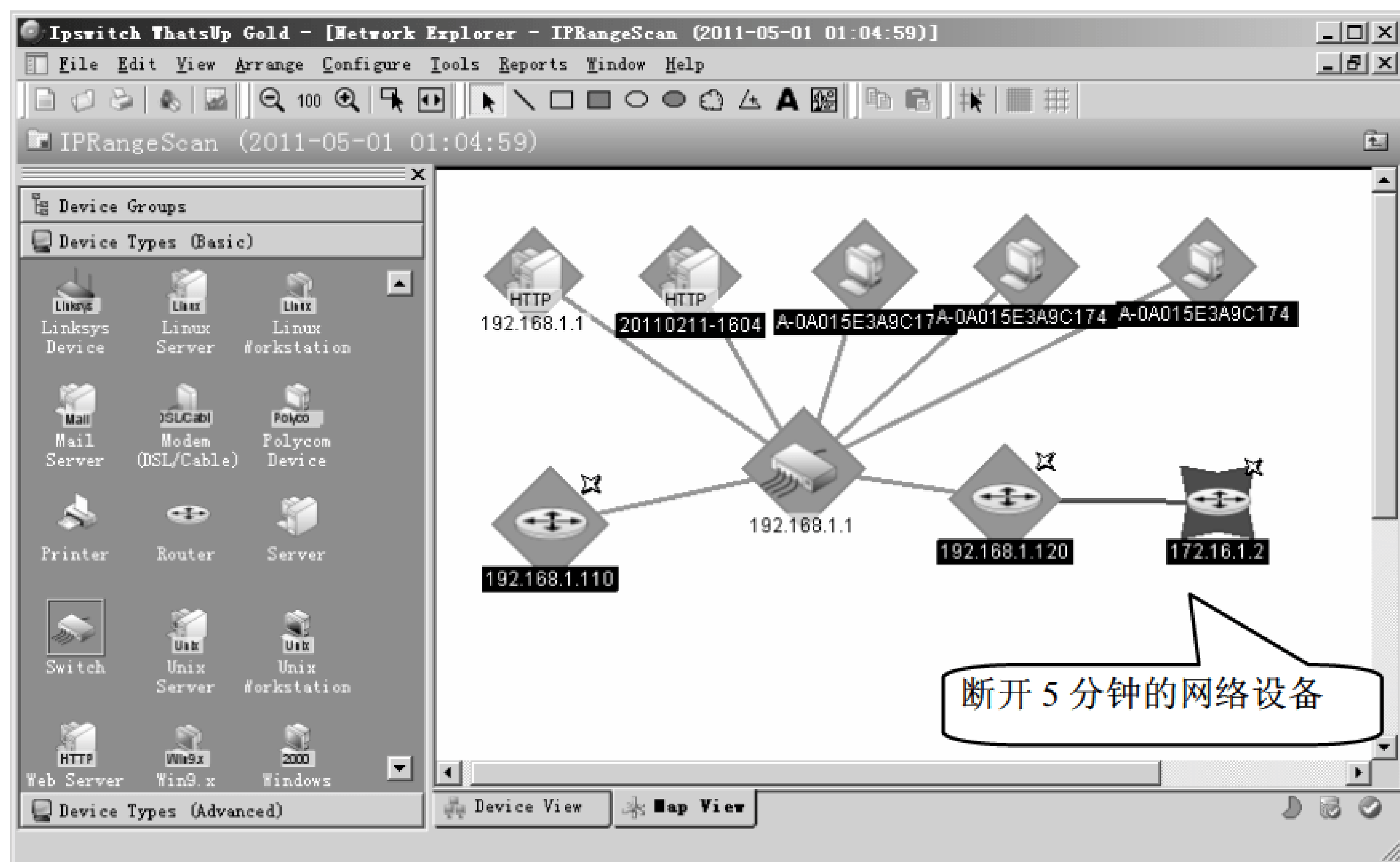


图 17-95　网络设备断开 5 分钟

（4）网络设备断开 15 分钟后，设备图标形状和颜色变化如图 17-96 所示。

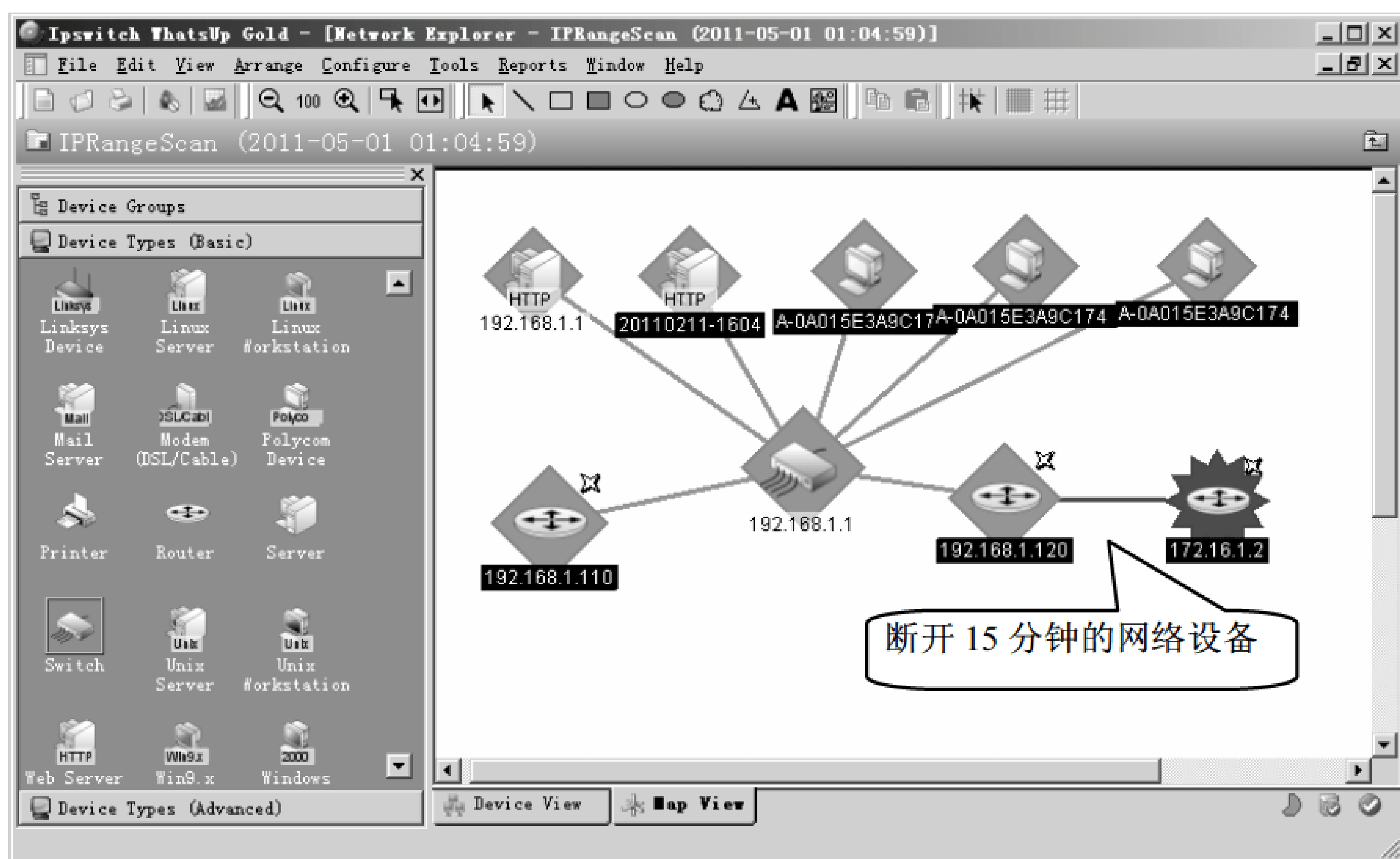


图 17-96　网络设备断开 15 分钟

在设备图标背景变化的同时，服务器会随之发出提示音，并向提前设定好的邮箱地址发送邮件。这类问题一般是网络线缆问题或网络设备问题，需要网络管理员排查检修。

网络故障排除的具体思路如下。

01 通过其他工具测试是否能与该设备通信，同时可以采用多种协议测试。通过测试结果判断故障问题，如果部分协议可通，可以考虑是否在网络中添加了访问策略。

02 通过其他方法依然无法连通时，要先考虑断开设备是否宕机，或作了配置调整，导致网络不可达。管理员可以到设备附近，调试配置设备。通过终端连接测试后设备运行没有问题，可排

除该故障。

03 网线在使用时也可能被损坏，可以使用测试工具对网线的连通作测试。

04 网线测试没有问题，也可能是网线接口故障，可以更换接口再作测试。

以上步骤只是通用步骤，可能在网络中出现特殊故障原因，管理员可以根据实际情况进行排查。

17.4 专家答疑

（1）使用网络管理平台监控、查看设备时，为什么不能获得设备的详细信息及性能？

答：可以从两个方面考虑出现这一现象的原因。其一，网络设备连接是否正常，可以通过网络测试工具，测试网络连接状态；其二，获取详细信息需要有网络管理协议的支持，可以查看被管设备是否安装、开启了 SNMP 网络管理协议，或者是 SNMP 协议使用的团体名是否一致，默认团体名为 public。

（2）使用 Spiceworks 网络管理平台监控网络时，网页内的部分信息无法显示，并且经常弹出如图 17-97 所示的提示框。

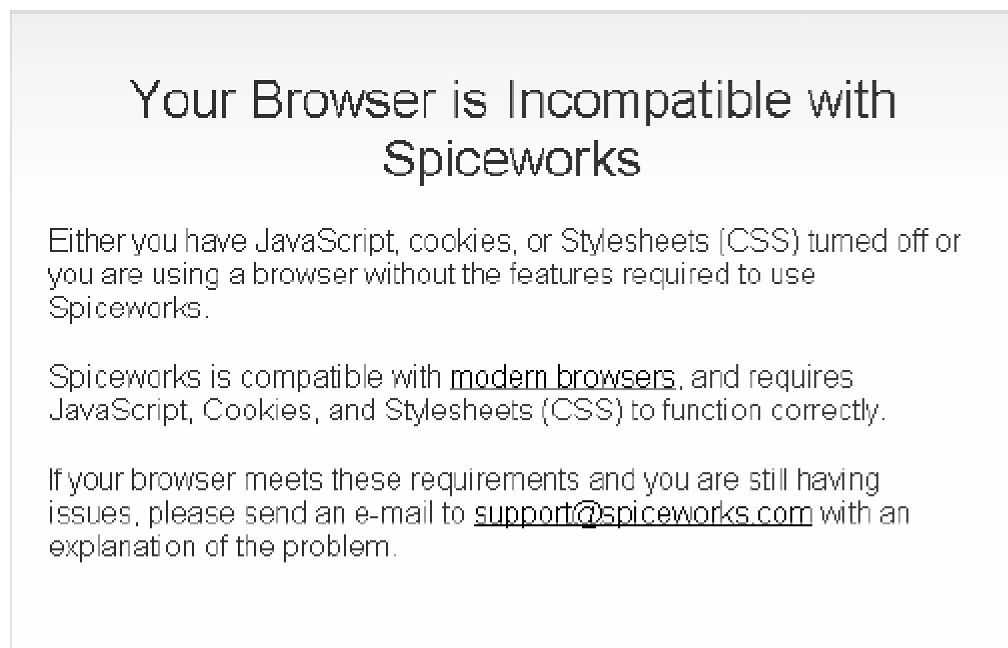


图 17-97　提示框

答：出现这类问题的主要原因是，使用 Spiceworks 网络管理平台查看信息时，网页中要显示动态信息，如果系统没有安装 JavaScript 环境或没有 CSS 文件，动态网页信息无法显示。所以在使用 Spiceworks 软件前，一定要先做好动态网页浏览环境。

第 18 章　网络流量监测分析

网络流量分析是指通过捕捉并分析网络中传输的数据包，掌握网络运行状况，有效帮助网络管理人员快速准确定位故障点，快速排查网络故障，从而提高网络性能，降低网络安全风险，增大网络可用性价值，确保整个网络的持续可靠运行。

18.1　网络流量分析的意义

网络流量监测主要是连续地采集网络中的数据包，通过对数据包进行分析，帮助网络管理员深入地了解网络的运行状况，发现网络中出现的问题，从而保证网络的服务质量。

通过对网络流量的分析，网络管理员可以详细地了解网络的运行状况。网络中的各种应用在运行的时候，每一个数据访问、每一个数据传输都要通过网络进行，通过分析网络数据包，可以清晰地了解应用程序的运行规律，从而帮助网络管理员更好地管理网络中的各种应用程序。同时网络中的每一个用户的网络行为都会影响到网络中的其他用户甚至整个网络的运行，每个用户的网络行为都会产生网络流量，通过对这些流量进行分析，可以清晰地检测到每个用户的具体网络行为，从而更好地对网络用户进行管理。

通过对网络流量的分析，网络管理员可以及时地发现网络出现的问题。任何网络异常，如网络用户的计算机感染了蠕虫病毒、中了后门程序等，都会产生异常的数据包，通过对数据包的长期分析就能及时发现网络用户的异常行为，从而提高解决问题的效率。

网络流量分析建立在深入了解网络的基础之上，通过对网络数据包的深入分析，及时发现网络流量中的异常数据包，可以帮助网络管理员及时解决网络故障，提高网络运行效率。

18.2　主流产品技术分析

要进行网络流量分析监测，除了要掌握扎实的网络基础知识外，还必须使用网络数据包嗅探工具。通过网络数据包嗅探工具捕捉网络中的数据包，然后对其进行分析。现在，主流的网络数据包嗅探工具有 Sniffer Pro 网络嗅探工具和科来网络分析系统等。

18.2.1 Sniffer Pro 网络嗅探工具概述

Sniffer Pro 网络嗅探工具是目前最为流行的网络嗅探工具之一。Sniffer 的主要功能是捕获网络数据，在大量的数据包中找到自己关心的数据包，然后分析解决问题。通过使用 Sniffer 嗅探工具，网络管理员可以判断在某个时间网络中的某个主机使用网络的具体行为，如该主机接收了多少数据包、发送了多少数据包、正在访问什么网站等信息，也可以判断整体网络的运行情况，如当前网络中运行了什么协议、哪个协议占用带宽过大、现在网络带宽使用率是多少等信息。因此，Sniffer 可以帮助管理员解决很多隐形的网络故障。

Sniffer 的安装位置选择非常重要，因为 Sniffer 只能捕捉到 Sniffer 所监听的网卡接收到的数据包，在不同的网络拓扑环境中，Sniffer 的安装位置不同。现在的网卡都有一个数据包识别功能，就是当网卡收到一个数据包的时候，会智能判断该数据包是不是发送给自己，只有当判定该数据包是发给自己的时候才会接收该数据包。如果要实现 Sniffer 监听网络数据包，必须将网卡处于“混杂模式”。所谓混杂模式，就是网卡可以接收所有发送给自己的数据包，不考虑该数据包中的目的地址是不是自己。下面详细讲解在不同的网络环境中 Sniffer 的安装位置。

集线器所连接的网络称为共享式以太网，共享式以太网中的数据通信依靠广播来完成，因此只要将主机的网卡设为混杂模式，也就意味着在网络的任何一个主机网卡都可以接收到网络中的所有数据包。在 Sniffer Pro 安装的计算机上，计算机的网卡会自动变成混杂模式。在集线器所连接的以太网中，Sniffer 的安装位置如图 18-1 所示。

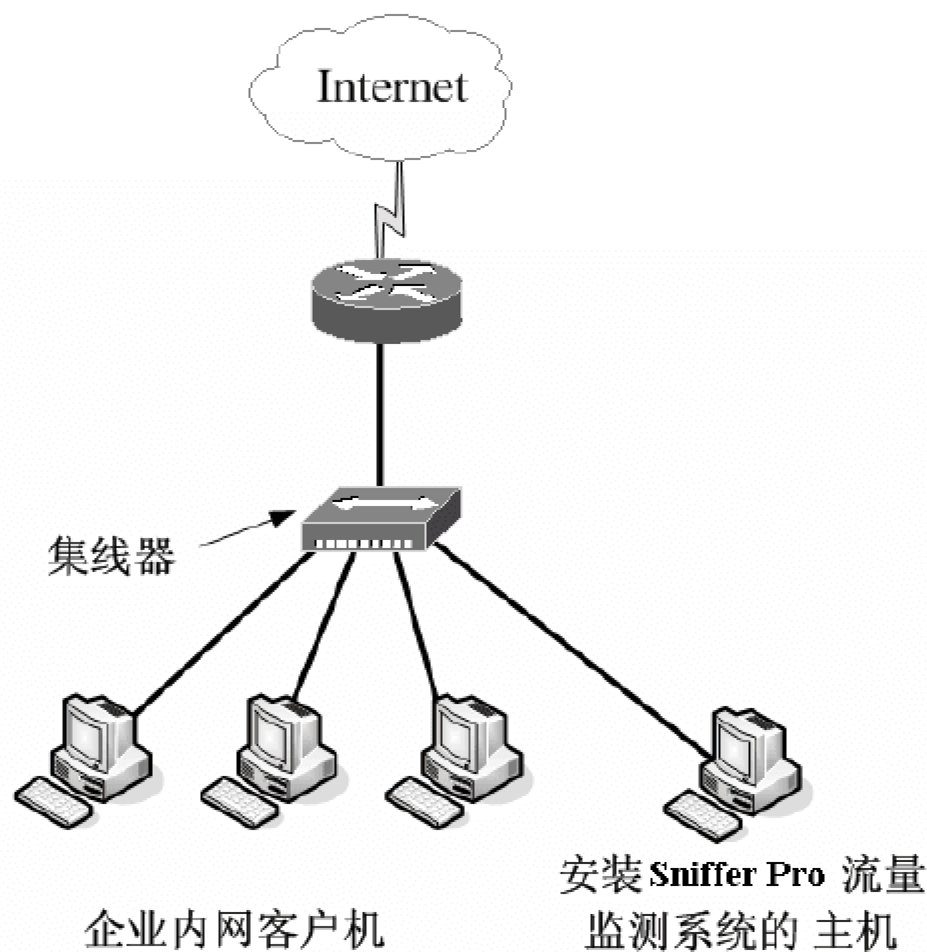


图 18-1　Sniffer 的安装位置拓扑图

交换机所连接的网络称为交换式以太网，交换式以太网中的数据通信是点到点通信，网络中的每个主机只接收发送给自己的数据包。在交换式以太网中，要想让 Sniffer 能够监听到网络中所有的数据包，可以有以下两种方法。

（1）在以太网中，如果使用的是网管级交换机连接路由器去连接互联网，要想让 Sniffer 监听到内部局域网和外部互联网的通信情况，可以在网管级交换机上配置端口镜像，并将网络设备的出口设置为目的端口，然后将 Sniffer 安装在连接在该端口的计算机上，就可以监听到整个网络。

镜像一般是将符合制定规则的报文复制到镜像目的端口。一般镜像目的端口会接入数据检测设备，用户利用这些设备对镜像过来的报文进行分析，进行网络监控和故障排除等。所谓端口镜像，就是把交换机一个或多个端口（VLAN）的数据镜像到一个或多个端口的方法。一般情况下，在这种以太网中为了实现对整个网络数据的监听，将交换机连接路由器（公司连接互联网用的路由器）的端口映射为 Sniffer 所在计算机连接的端口，如图 18-2 所示。需要注意的是，不一样的交换设置方法不同，这里简单介绍下 Cisco 交换端口镜像设置方法。

```
Router#configure terminal
//进入全局配置模式
Router(config)#monitor session 2 source interface g1/0/1
//指定端口镜像进程和侦听源端口（g1/0/1）
Router(config)#monitor session 2 destination g1/0/2
//指定端口镜像进程和侦听目标端口（g1/0/2）
```

（2）在以太网中，如果使用的是交换机连接代理服务器连接以太网。在这种网络拓扑结构中，内部局域网所有的数据包，可以将 Sniffer 安装在代理服务器（代理内部局域网访问互联网的主机）上。Sniffer 的安装位置如图 18-3 所示。

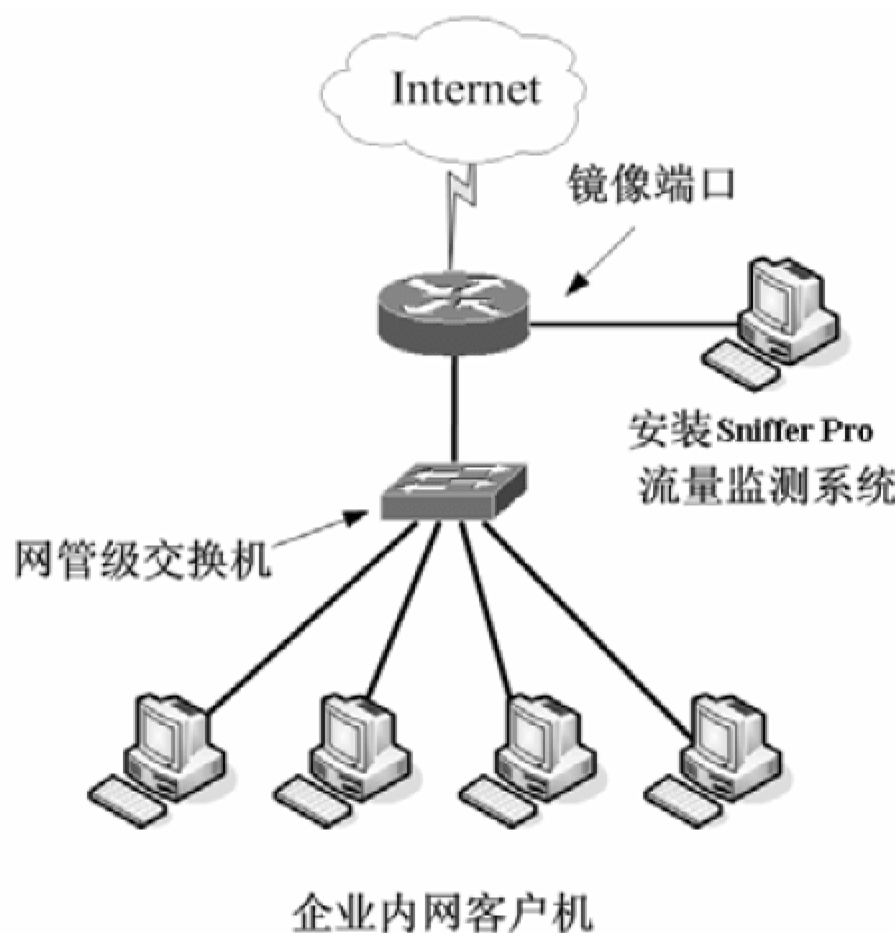


图 18-2　使用镜像端口监管流量

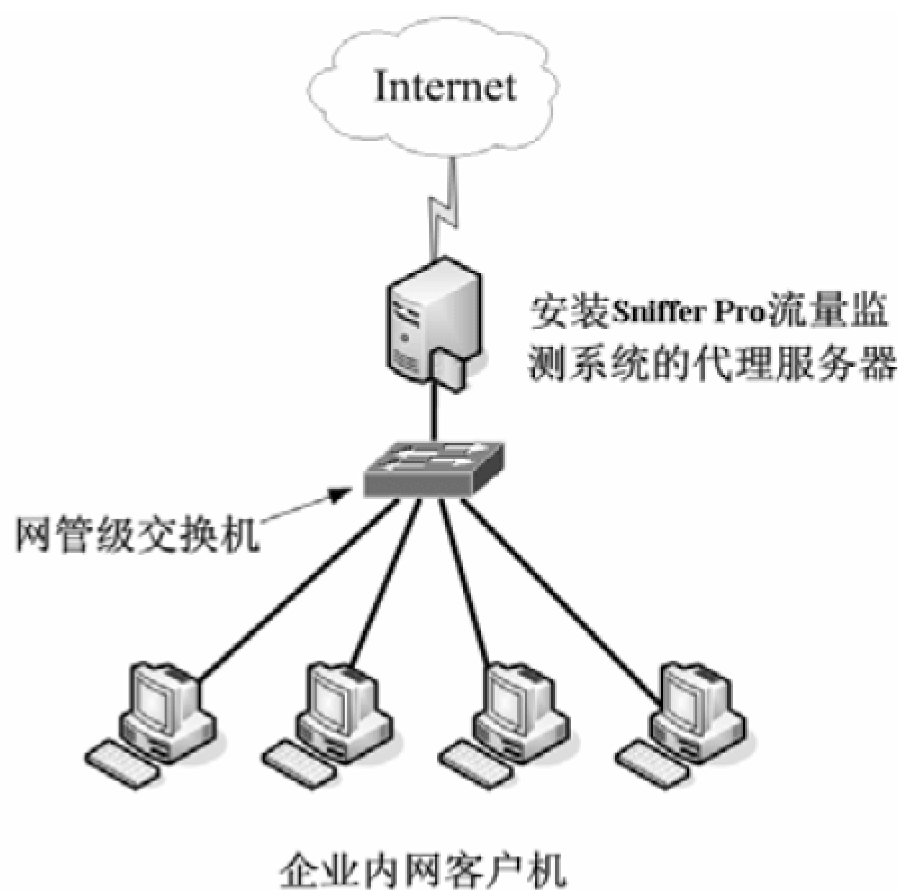


图 18-3　Sniffer 安装在代理服务器上

18.2.2　科来网络分析系统

科来网络分析系统是一个集数据包采集、解码、协议分析、统计、图表、报表等多种功能为一体的综合网络分析平台。它可以帮助网络管理员排查网络安全隐患、网络流量监控、定位网络故障。

与 Sniffer Pro 嗅探工具不同，科来网络分析系统是由我国自主研发并拥有全部知识产权的网络分析产品。它可以为网络管理工作提供全面可靠的数据依据，可以帮助用户排查网络故障、规避网络风险、提升网络性能、提高故障处理能力、减少故障损失并降低管理成本，所以，科来网络分析系统是网络管理中的必备产品。

科来网络分析系统能够让网络管理者在遇到各种网络问题的时候，轻松找到解决办法，对网络中监测到的数据进行分析、诊断，从而帮助网络管理人员及时排除网络故障，规避网络安全风险，

提高网络性能。

使用科来网络分析系统，网络管理者不用再担心遇到网络故障无法解决，因为科来网络分析系统成熟的数据包分析机制可以帮助企业把网络故障和安全风险降到最低，网络性能会逐步得到提升。总体上来说，科来网络分析系统可以帮助管理员快速地查找和排除网络故障，及时找到网络瓶颈提升网络性能，并且科来网络分析系统能够分析各种网络协议，从而更好地管理资源，提高网络应用质量。

科来网络分析系统整合了行业领先的专家分析技术，对当前复杂的网络提供精确分析，在网络安全、网络性能、网络故障方面提供最全面而深入的数据依据，是企业、政府、学校等网络管理所需要的关键性产品。

18.3 科来网络分析系统的安装与使用

科来网络分析系统和 Sniffer Pro 一样，安装位置特别重要，应该安装在网络的节点处以便能够捕获到需要的数据包，可根据上文中 Sniffer Pro 的讲解选择科来网络分析系统的安装位置。下面介绍科来网络分析系统的安装与使用方法。

18.3.1 安装科来网络分析系统

安装科来网络分析系统的具体操作步骤如下。

01 双击科来网络分析系统安装文件，弹出【欢迎您使用科来网络分析系统 2010 技术交流版、安装程序】对话框，单击【下一步】按钮，如图 18-4 所示。

02 弹出【使用许可协议】对话框，选中【我接受本协议】单选按钮，单击【下一步】按钮，如图 18-5 所示。

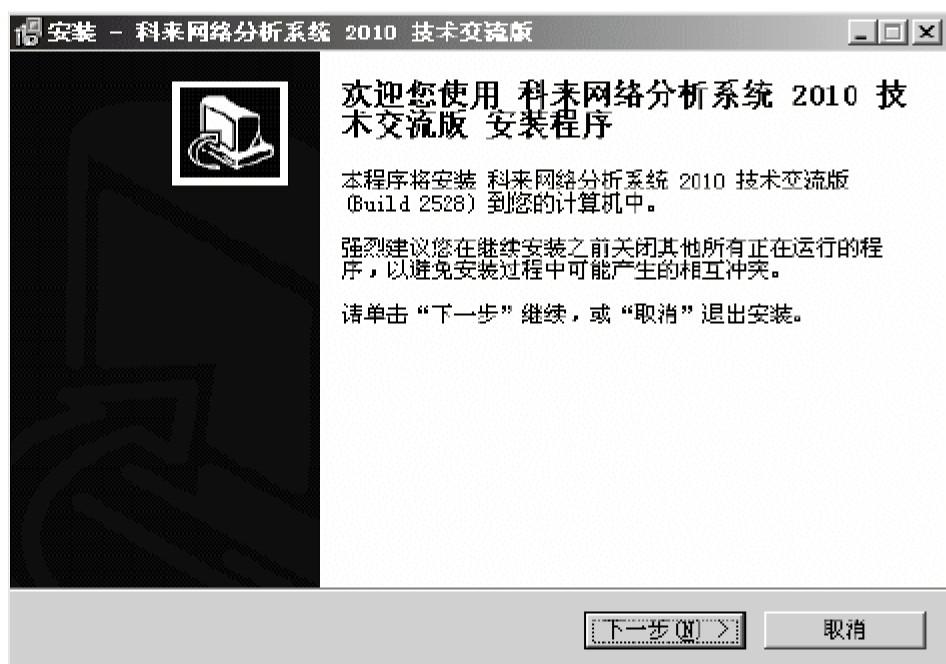


图 18-4　安装向导对话框

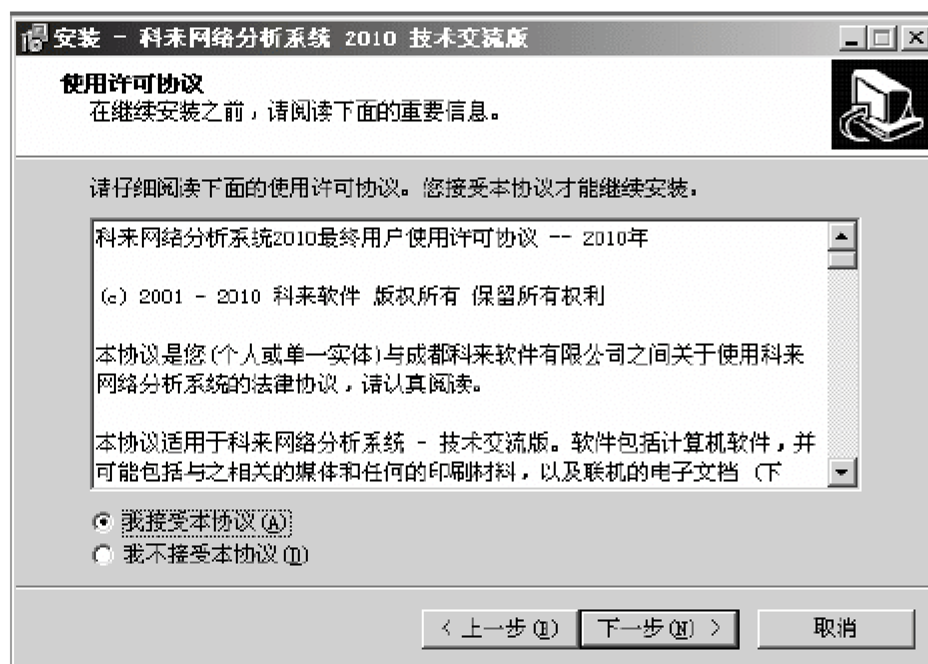


图 18-5　【使用许可协议】对话框

03 弹出【信息】对话框，显示科来网络分析系统更新信息，单击【下一步】按钮，如图 18-6 所示。

04 弹出【选择目标文件夹】对话框，可以单击【浏览】按钮自定义安装路径，本实例采用默认路径，单击【下一步】按钮，如图 18-7 所示。

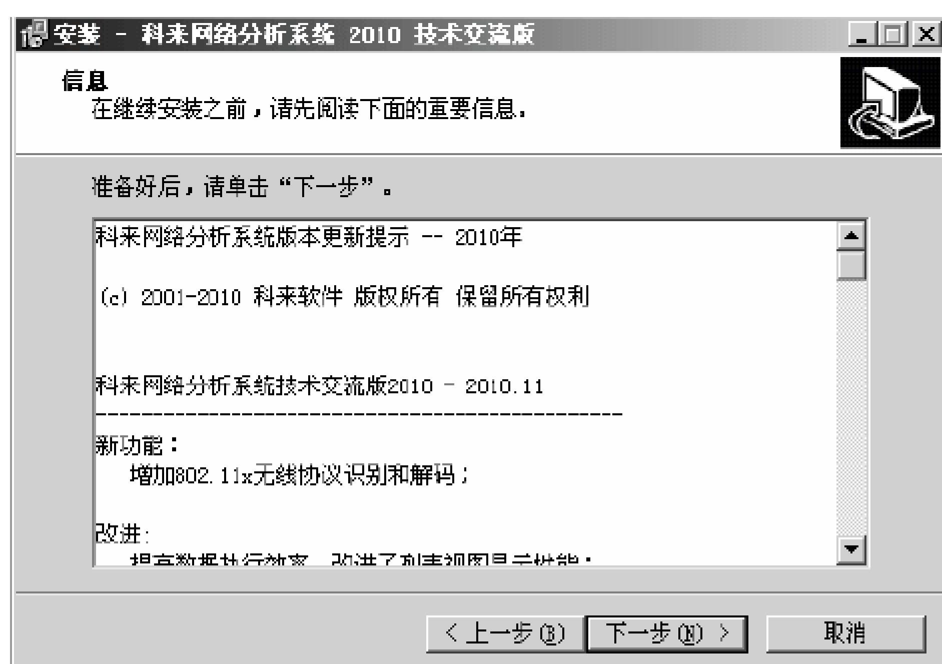


图 18-6 【信息】对话框

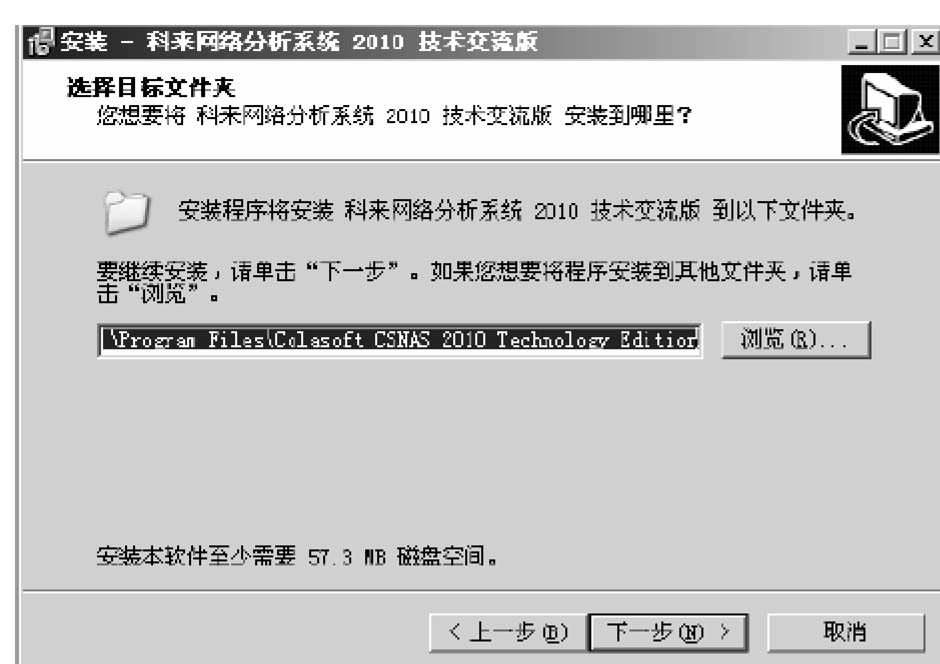


图 18-7 【选择目标文件夹】对话框

05 弹出【选择组件】对话框，默认选择安装所有组件，单击【下一步】按钮，继续安装科来网络分析系统，如图 18-8 所示。

06 弹出【选择开始菜单文件夹】对话框，可以单击【浏览】按钮自定义科来网络分析系统的快捷方式安装路径，单击【下一步】按钮，如图 18-9 所示。

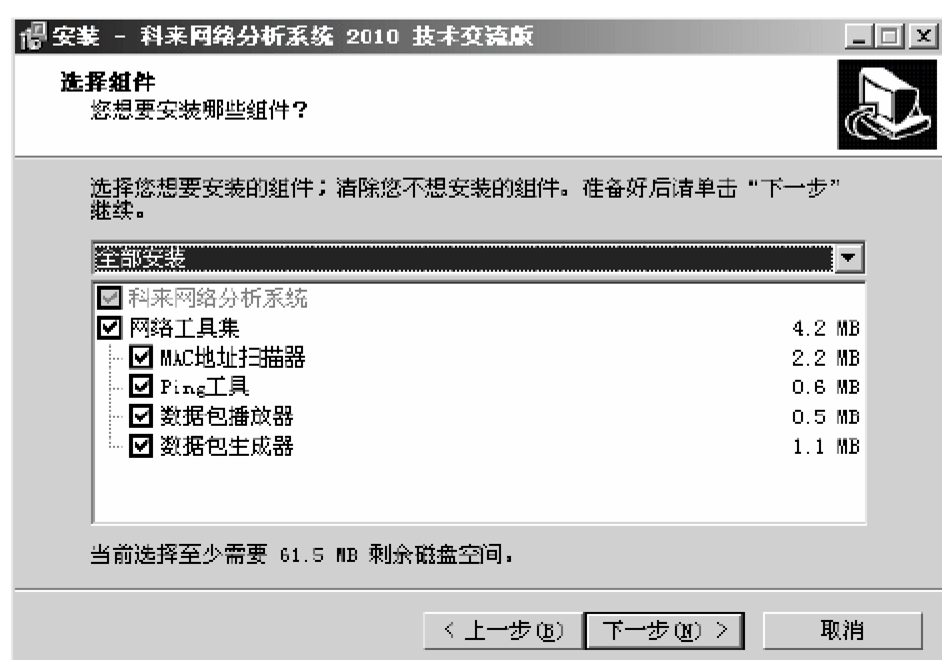


图 18-8 【选择组件】对话框

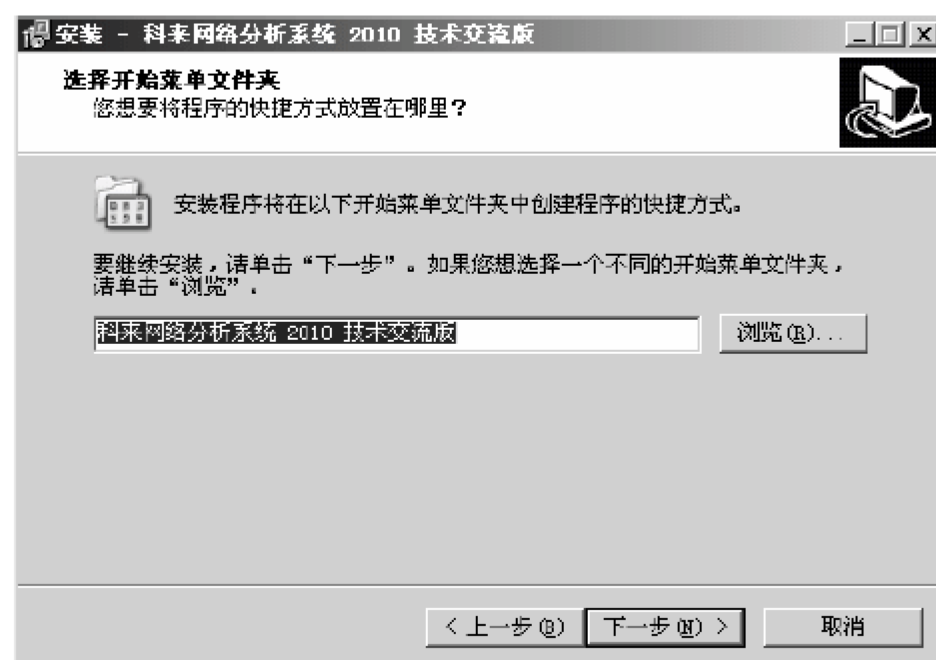


图 18-9 【选择开始菜单文件夹】对话框

07 弹出【选择附加任务】对话框，选中【创建桌面图标】和【创建快速启动图标】复选框，单击【下一步】按钮，如图 18-10 所示。

08 弹出【准备安装】对话框，显示了科来网络分析系统的安装信息，确认无误后，单击【安装】按钮，如图 18-11 所示。

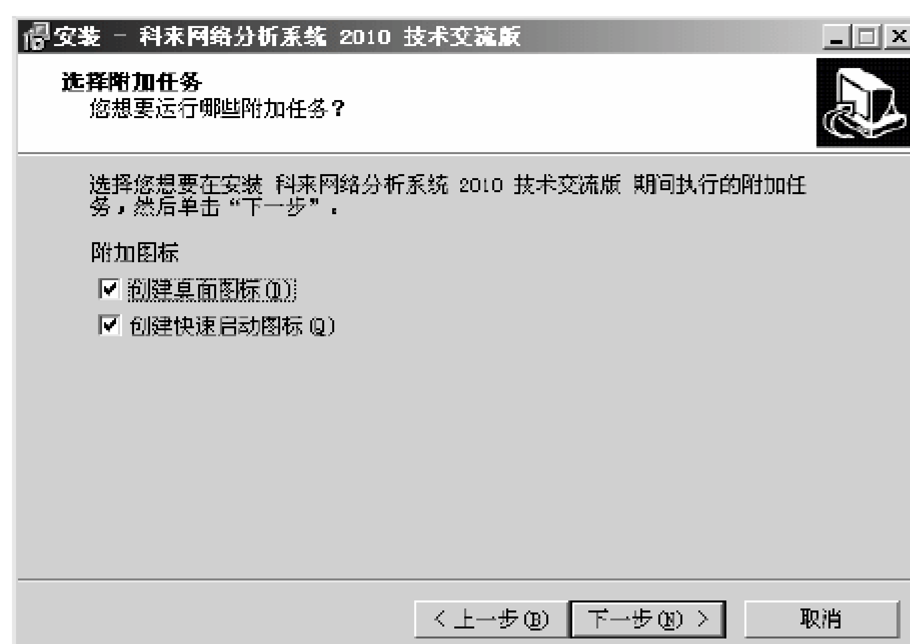


图 18-10 【选择附加任务】对话框

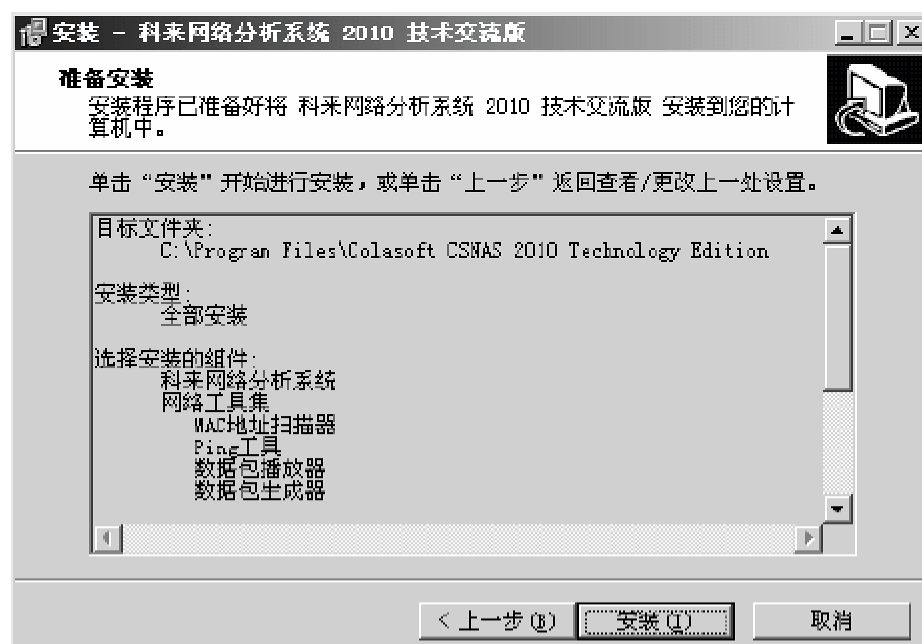


图 18-11 【准备安装】对话框

09 科来网络分析系统安装正在继续并显示安装进度，如图 18-12 所示。

10 安装的过程中会弹出【信息】对话框，显示科来网络分析系统信息，单击【下一步】按钮，如图 18-13 所示。



图 18-12　安装进度对话框

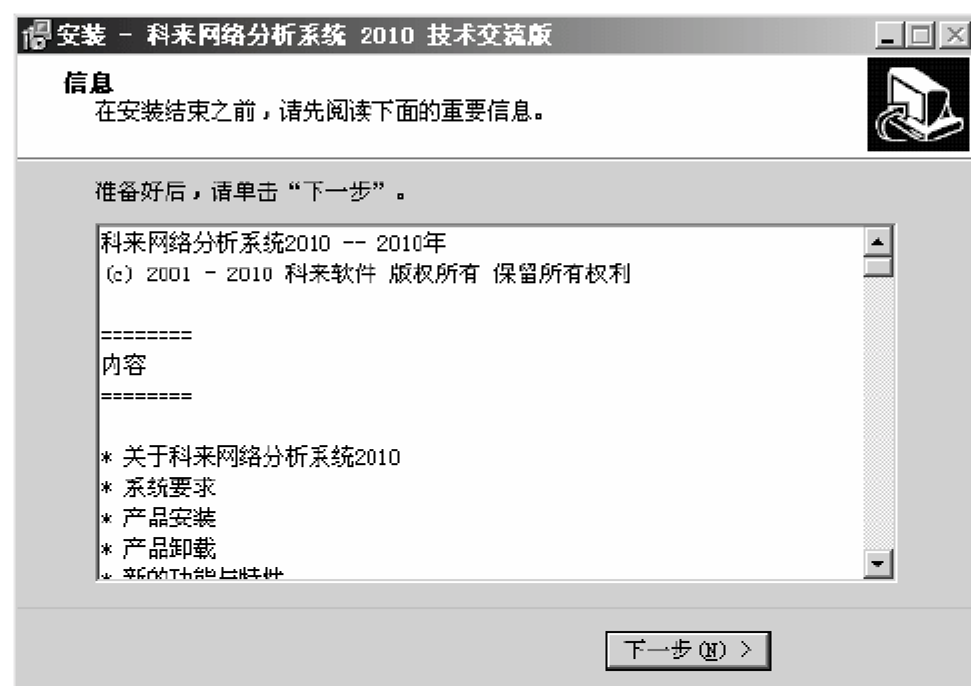


图 18-13　【信息】对话框

11 单击【完成】按钮，结束科来网络分析系统的安装，如图 18-14 所示。

12 选择【开始】➢【所有程序】➢【科来网络分析系统 2010 技术交流版】➢【科来网络分析系统 2010 技术交流版】命令，打开科来网络分析系统。在【用户名】和【公司】文本框中分别输入用户名和公司信息，本实例中输入用户名为“sushi”，公司为“howin”，在【序列号】文本框中输入科来网络分析系统的序列号，序列号可以通过单击【点击这里获取序列号】超链接在线获得，单击【下一步】按钮，如图 18-15 所示。



图 18-14　完成安装向导



图 18-15　科来产品注册对话框

13 弹出【请阅读以下重要信息】对话框，在其中显示了科来网络分析信息激活信息，单击【下一步】按钮，激活科来网络分析系统，如图 18-16 所示。

14 科来网络分析系统激活成功，单击【完成】按钮，如图 18-17 所示。

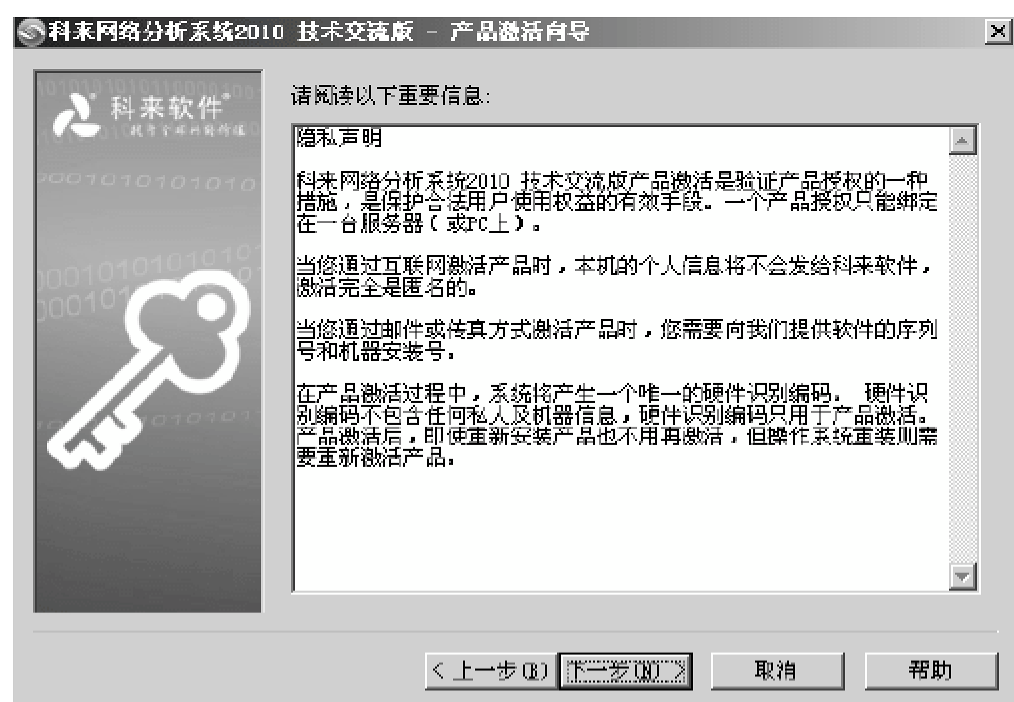


图 18-16　【请阅读以下重要信息】对话框



图 18-17　激活产品成功对话框

15 完成激活后，自动打开科来网络分析系统程序主界面，至此科来网络分析系统安装并激活完成，如图 18-18 所示。



图 18-18　科来网络分析系统程序主界面

18.3.2　设置过滤器

默认情况下，科来网络分析系统捕捉监听网卡监听到的所有数据包，每次捕捉到的数据包量比较大，不利于提高分析效率。而过滤器就是对捕捉到的数据包进行过滤，通过设置数据包过滤器可以减少捕捉到的数据包的数量，减少数据包的分析时间，提高数据包的分析效率，从而加快解决网络故障的速度。

设置过滤器的具体操作步骤如下。

01 选择【开始】➢【所有程序】➢【科来网络分析系统 2010 技术交流版】➢【科来网络分析系统 2010 技术交流版】命令，打开科来网络分析系统，选中监听网卡【本地连接】复选框，单击右侧【设置捕捉过滤器】链接，如图 18-19 所示。



图 18-19　科来网络分析系统

02 弹出【过滤器】对话框，默认情况下没有设置过滤器，则监听所有数据包，如图 18-20 所示。

03 选中 ARP/RARP 协议【接受】复选框，表明要捕捉关于 ARP/RARP 协议的数据包，单击下方的按钮，如图 18-21 所示。

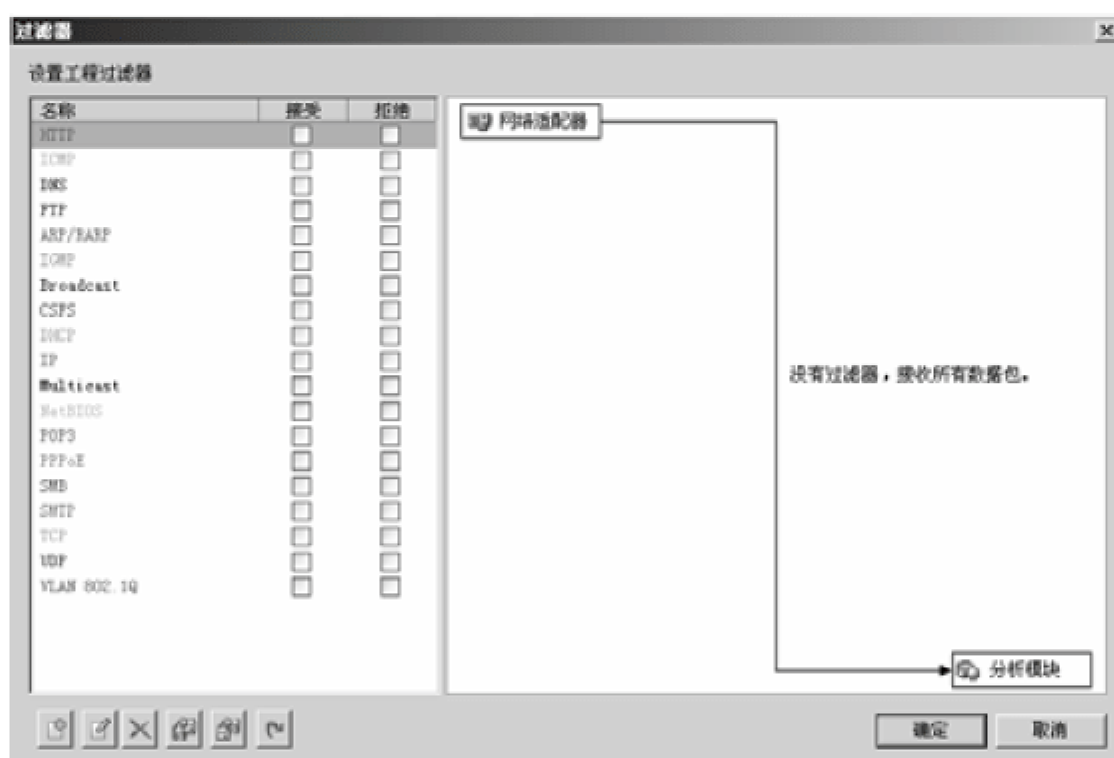




图 18-20　【过滤】对话框　　　图 18-21　选择数据包过滤规则

04 弹出【数据包过滤器】对话框，在其中设置更加精确的数据包捕捉过滤器。在【名字】文本框中输入过滤器的名称“过滤 1”，选中【地址规则】复选框，在【地址 1】下拉列表中选择【IP 地址】选项，输入【IP 地址】为“172.16.4.1”，在【地址 2】下拉列表中选择【任意地址】选项，在【方向】下拉列表中选择【地址 1<->2】选项，表明只捕捉源 IP 为 172.16.4.1 的数据包，单击【确定】按钮，如图 18-22 所示。

05 返回【过滤器】对话框，选中【过滤 1】复选框，表明使用【过滤 1】过滤器进行数据包过滤，单击【确定】按钮，如图 18-23 所示。

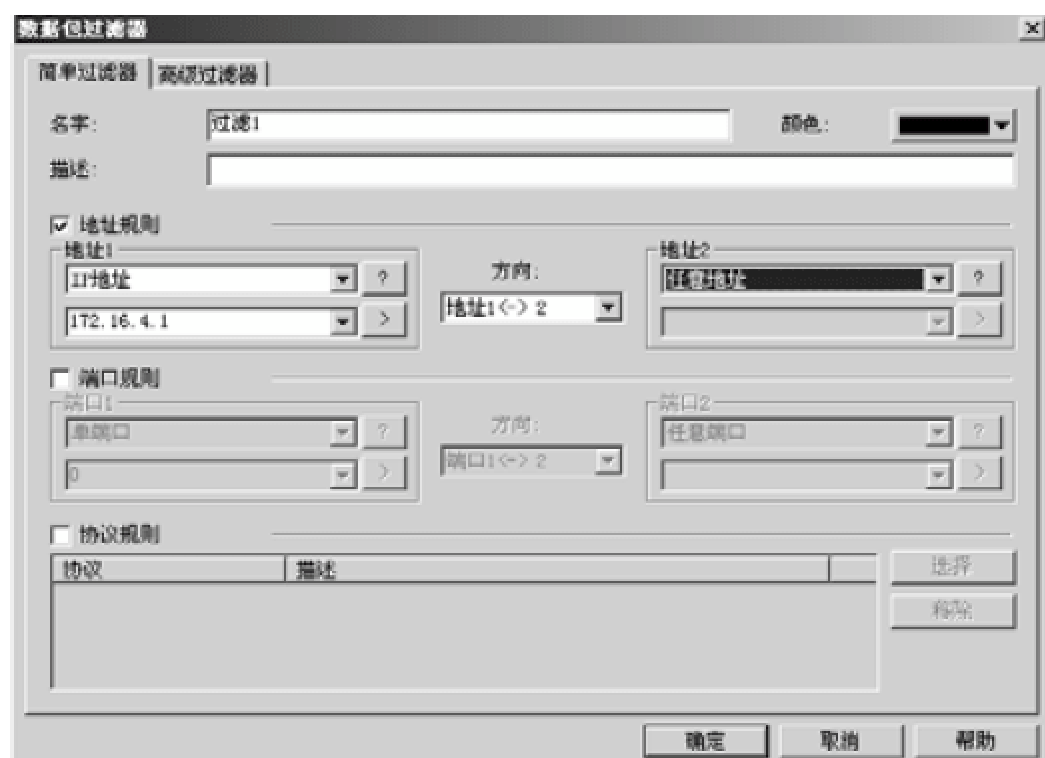


图 18-22 【数据包过滤器】对话框

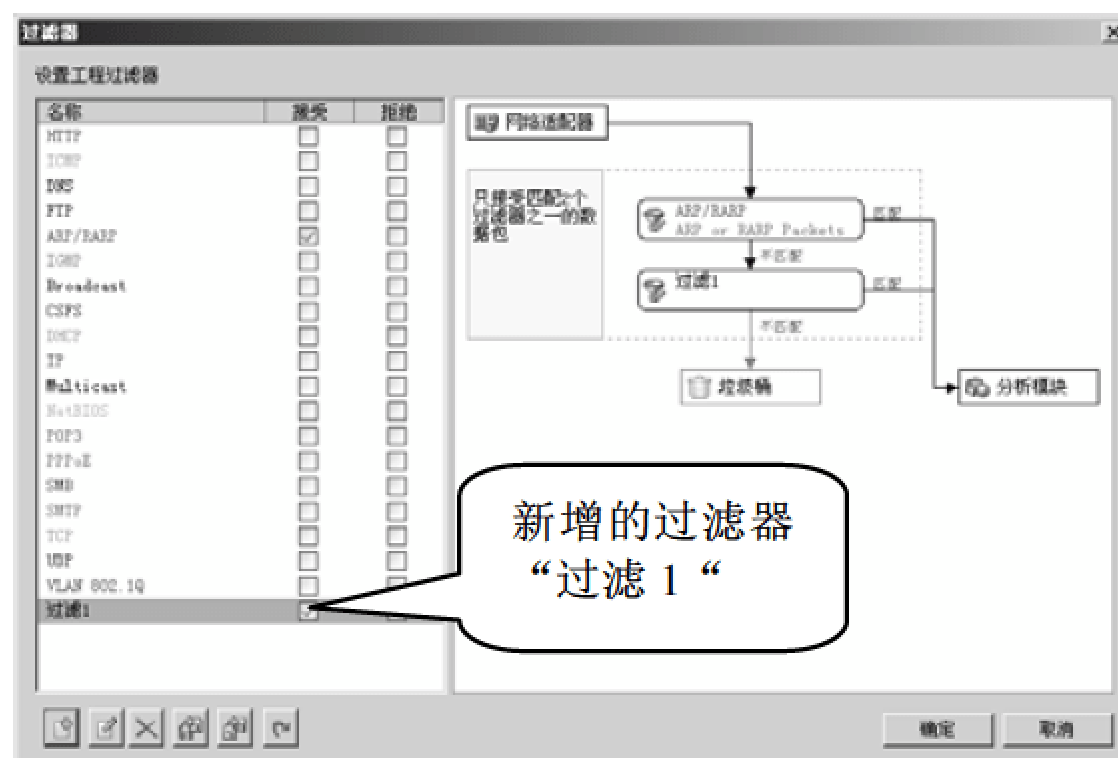


图 18-23 【过滤器】对话框

06 返回至科来网络分析系统的主程序界面，在右侧会看到捕捉过滤器为【已选择 2 个接受过滤器，只接受匹配的数据包】，表明设置捕捉过滤器成功，如图 18-24 所示。



图 18-24 科来网络分析系统的主程序界面

18.3.3 使用科来网络分析系统分析 ARP 异常

局域网通信依赖大量的 ARP 广播，但是很多病毒或者木马就趁机利用 ARP 广播进行 ARP 攻击，严重影响局域网的畅通。

利用科来网络分析系统分析网络中 ARP 异常的具体操作步骤如下。

01 选择【开始】➢【所有程序】➢【科来网络分析系统 2010 技术交流版】➢【科来网络分析系统 2010 技术交流版】命令，打开科来网络分析系统，选中监听网卡【本地连接】复选框，单击右侧【设置捕捉过滤器】链接。

02 弹出【过滤器】对话框，选中 ARP/RARP 协议的【接受】复选框，表明要捕捉关于 ARP/RARP 协议相关的数据包，单击【确定】按钮。

03 返回至科来网络分析系统程序主界面，单击右下角【开始】按钮，开始数据捕捉，如

图 18-25 所示。



图 18-25 科来网络分析系统程序主界面

04 单击【停止】按钮，可以结束数据的捕捉，如图 18-26 所示。

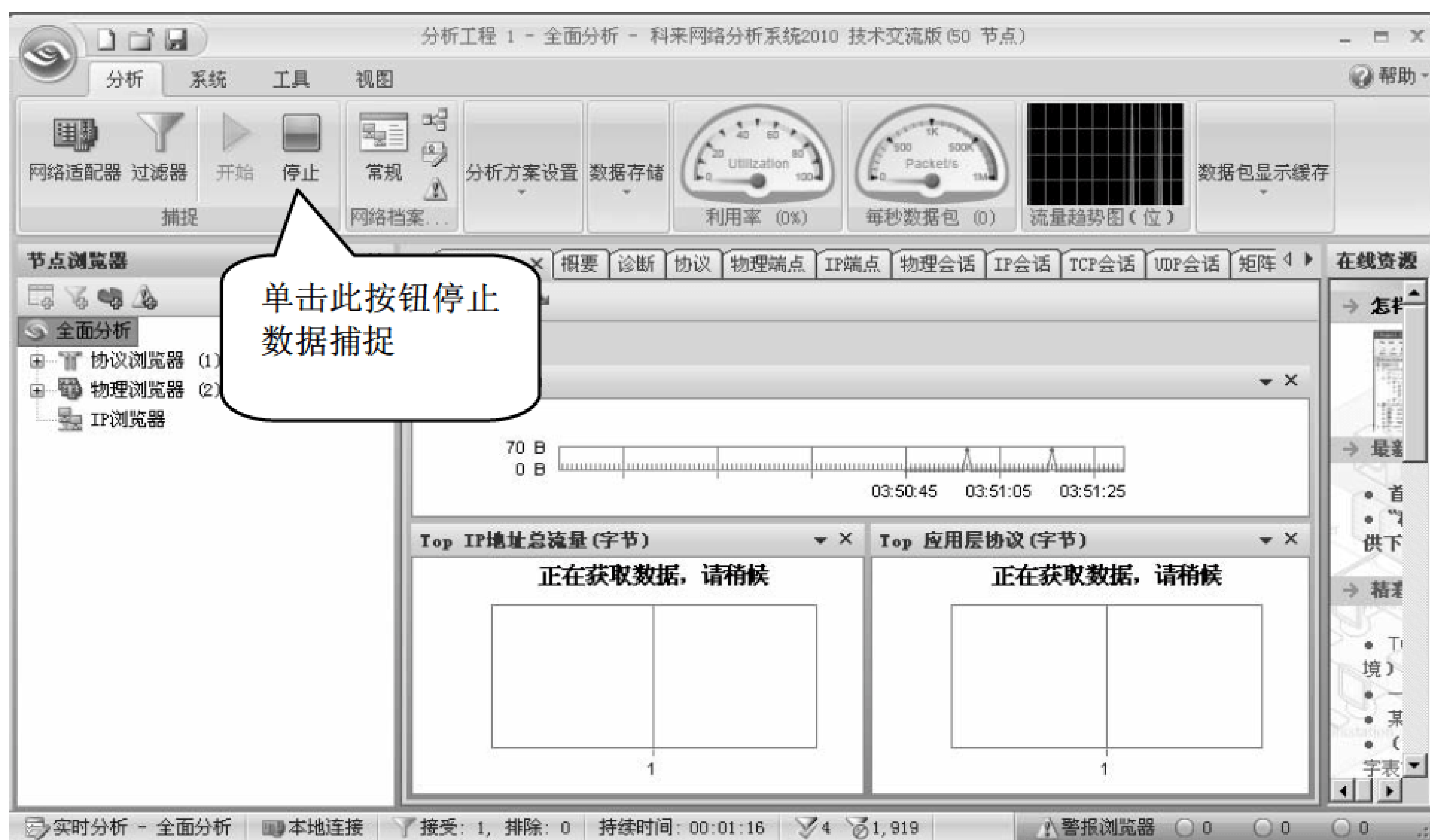


图 18-26 结束数据捕捉

05 当数据捕获完成后，选择【协议】选项卡，在该窗口中可以看到网络中各个协议的使用比例情况，如果 ARP 协议使用比例较大，则可以怀疑网络是否中了 ARP 病毒或者某台主机正在进行 ARP 攻击，如图 18-27 所示。

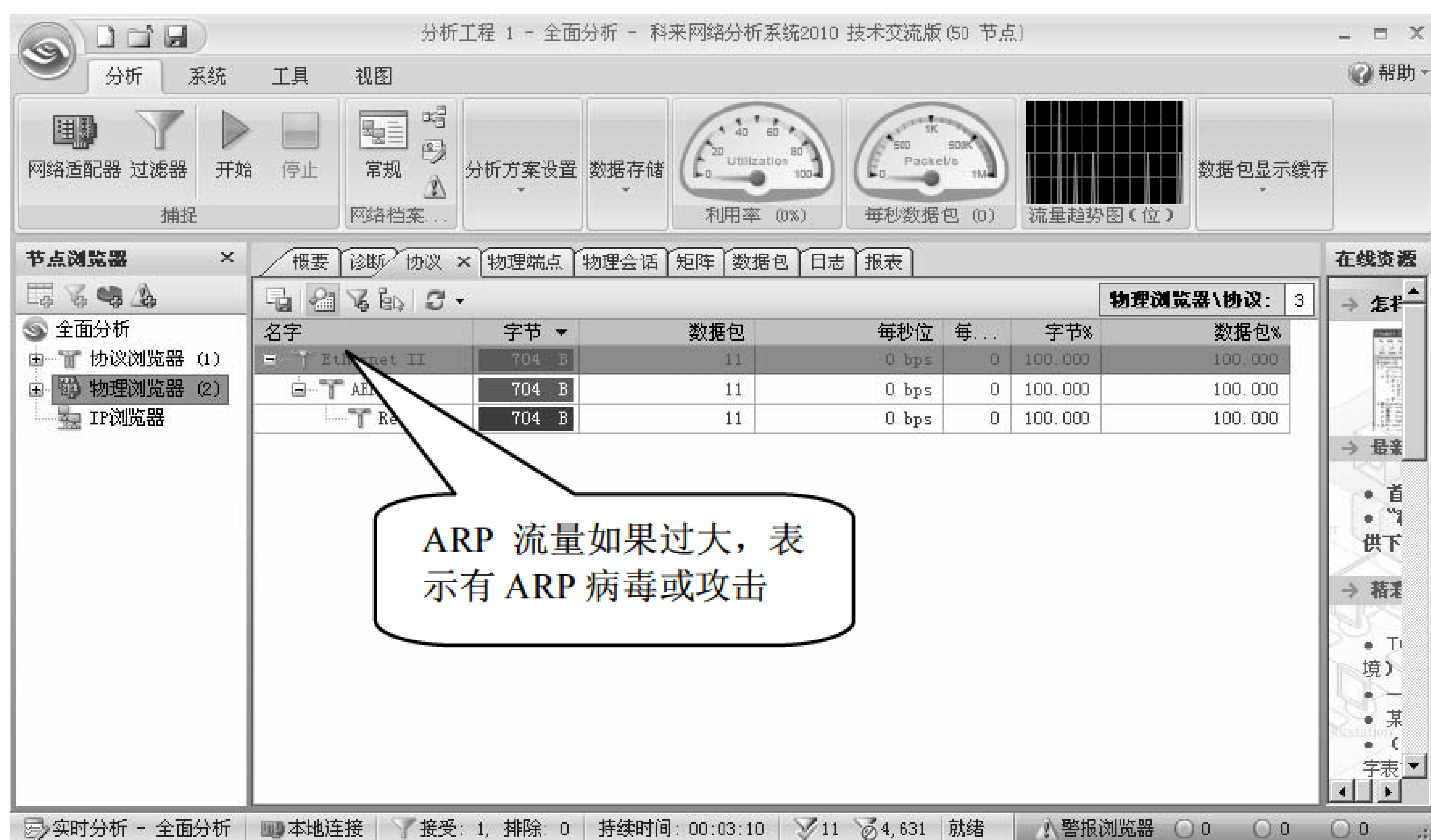


图 18-27 【协议】选项卡

06 选择【数据包】选项卡，在打开的界面中可以查看科来网络分析系统捕捉到的数据包。从捕获结果中可以看出，在网络中哪些主机在进行 ARP 广播，如果发现某个主机一直和大量的主机进行 ARP 通信，则可以怀疑该主机正在进行 ARP 攻击，如图 18-28 所示。

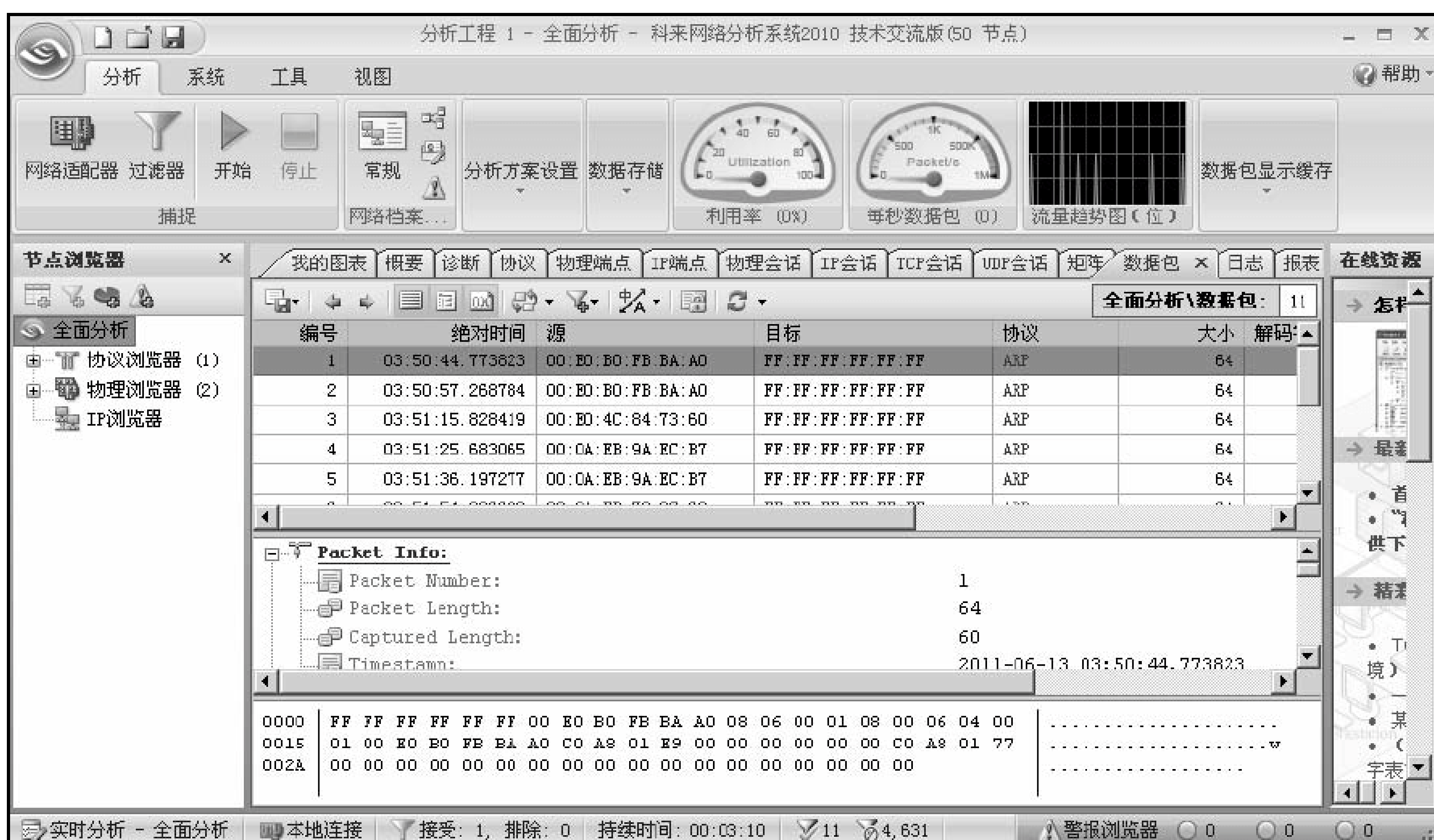


图 18-28 【数据包】选项卡

18.4 项目实战：使用 Sniffer Pro 进行网络流量监控分析

Sniffer Pro 的主要功能是捕获数据包并进行分析，网络管理人员可以通过对捕获到的数据包进行分析，从而得到网络的运行情况。Sniffer Pro 提供的多种仪表盘可以帮助网络管理人员更加直观地获取网络中协议、计算机之间通信等运行信息，从而帮助网络管理人员及时解决网络故障。

18.4.1　安装 Sniffer Pro 网络嗅探工具

安装 Sniffer Pro 网络嗅探工具的具体操作步骤如下。

01 运行安装程序，弹出 Sniffer Protable 对话框，单击 Next 按钮，如图 18-29 所示。

02 弹出 Setup 提示框，Sniffer 安装正在继续，如图 18-30 所示。

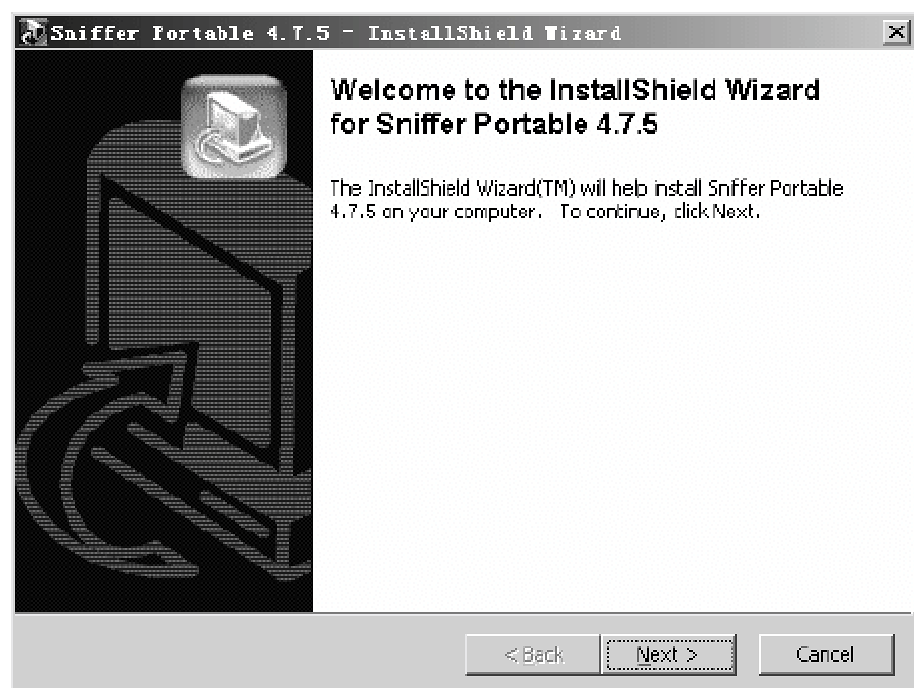


图 18-29　Sniffer Protable 对话框

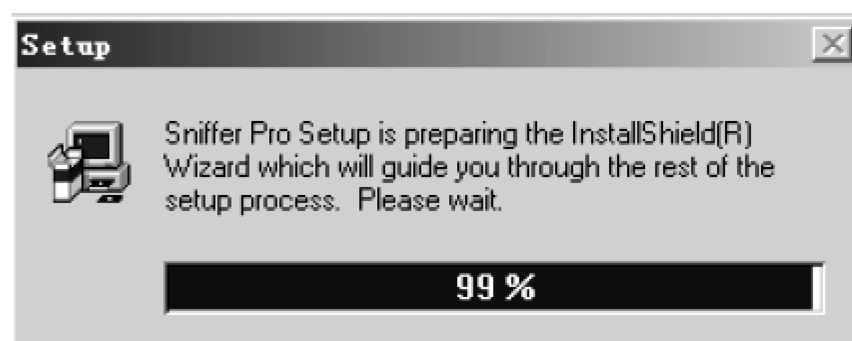


图 18-30　Setup 提示框

03 弹出 Welcome 对话框，单击 Next 按钮，如图 18-31 所示。

04 弹出 Software License Agreement 对话框，单击 Yes 按钮，表示同意 Sniffer Pro 的安装协议，如图 18-32 所示。



图 18-31　Welcome 对话框

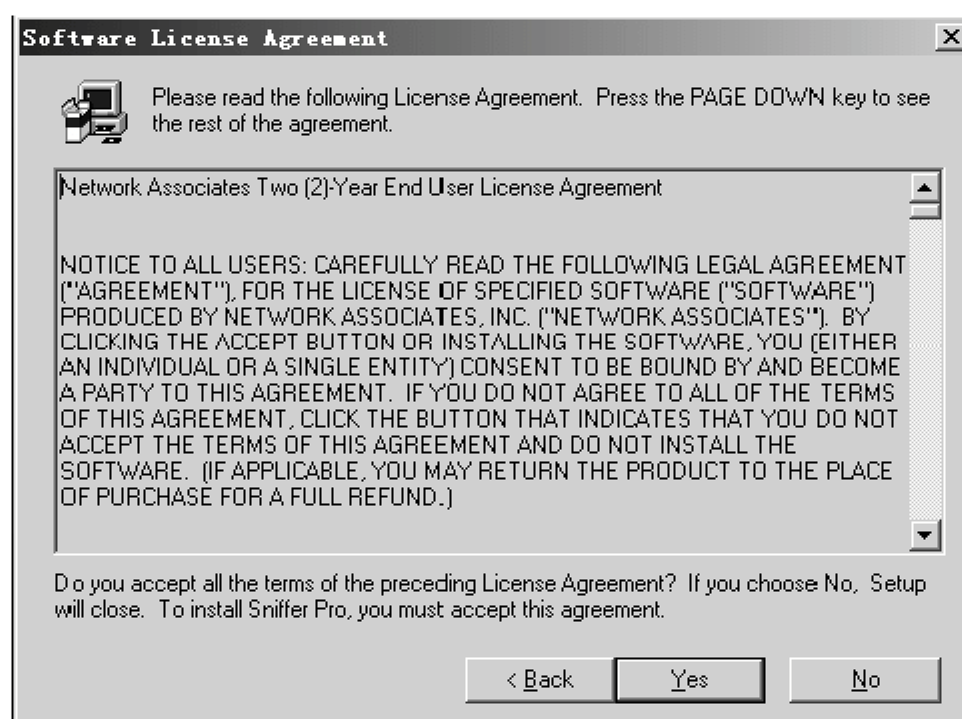


图 18-32　Software License Agreement 对话框

05 弹出 User Information 对话框，在 Name 和 Company 文本框中分别输入用户的姓名和公司信息，本实例中输入姓名为“sushi”，公司为“yingda”，单击 Next 按钮，如图 18-33 所示。

06 弹出 Choose Destination Location 对话框，单击 Browse 按钮选择 Sniffer 的安装路径，默认安装路径为“C:\Program Files\NAI\SnifferNT”，单击 Next 按钮，如图 18-34 所示。

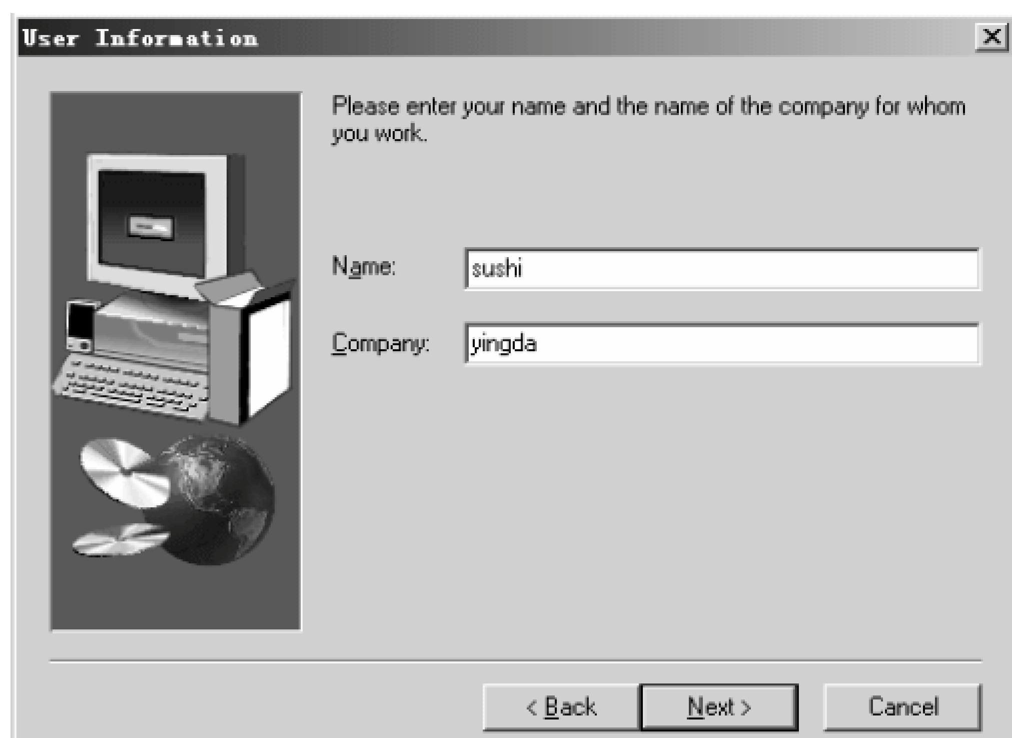


图 18-33　User Information 对话框



图 18-34　Choose Destination Location 对话框

07 弹出 Sniffer Pro User Registration(Sniffer Pro 用户注册)对话框，在 First Name、Last Name、Business、Customer 和 E-mail 文本框中输入相关信息，注意图 18-35 所示的每个文本框必须输入必要的信息，单击【下一步】按钮。

08 弹出 Sniffer Pro User Registration 对话框，在 Address（地址）、City（城市）、Country（国家）、Postal（邮编）、Phone（电话）和 Fax Number（传真号码）文本框中输入相关信息，单击【下一步】按钮，如图 18-36 所示。





图 18-35　Sniffer Pro User Registration 对话框　　图 18-36　Sniffer Pro User Registration 对话框

09 弹出 Sniffer Pro User Registration 对话框，在 Please let us know where you heard about this product（请让我们知道你是在哪里听到关于这个产品的信息）文本框中选择用户是通过什么渠道获得关于 Sniffer 的信息，在 Do you wish to receive announcements about this product（你是否希望接受关于这个产品的广告）文本框中选择是否愿意接收和 Sniffer 有关的广告，在 May we share your name with other companies that use NAI products（我们是否可以和其他公司分享你使用这个产品的信息)文本框选择是否愿意让其他的公司知道你们正在使用 Sniffer，在 Sniffer Serial Number(Sniffer 序列号）文本框中输入 Sniffer 的产品密钥，单击【下一步】按钮，如图 18-37 所示。

10 弹出 Sniffer Pro User Registration 对话框，选择用户如何接入互联网的，有三个选项，分别为 Direct Connection to the Internet（直接接入互联网）、Connection to the Internet through a Proxy（通过代理接入互联网）和 Not connected to network or Dial-up Print & fax option（没有接入互联网或者通过电话和传真接入互联网）。这里选择没有接入互联网，单击【下一步】按钮，如图 18-38 所示。

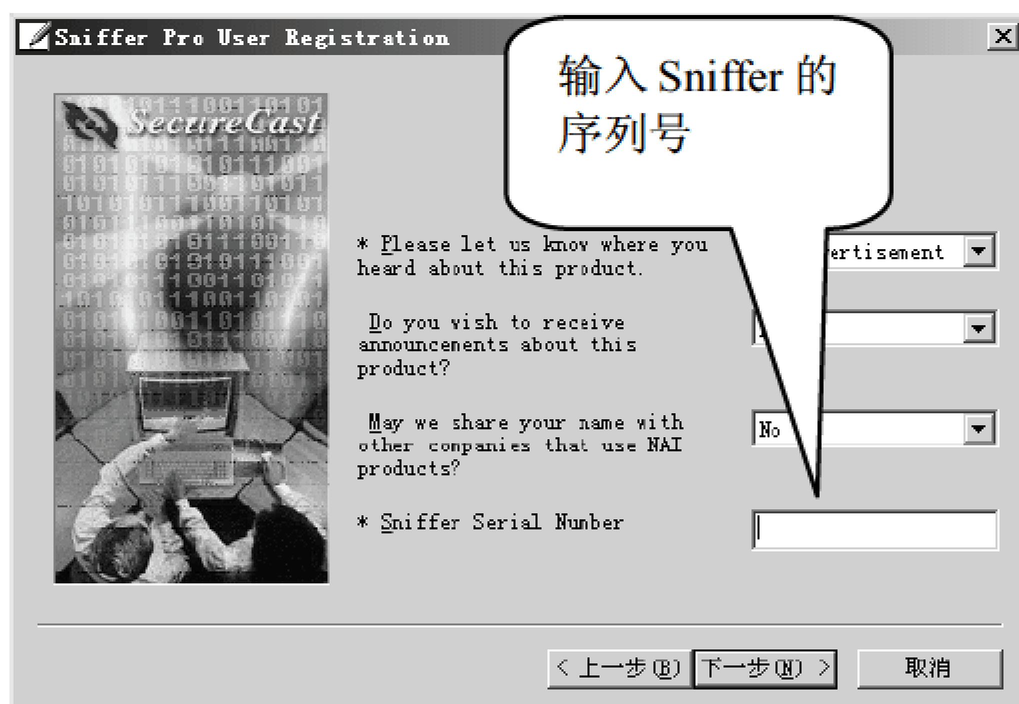


图 18-37　Sniffer Pro User Registration 对话框

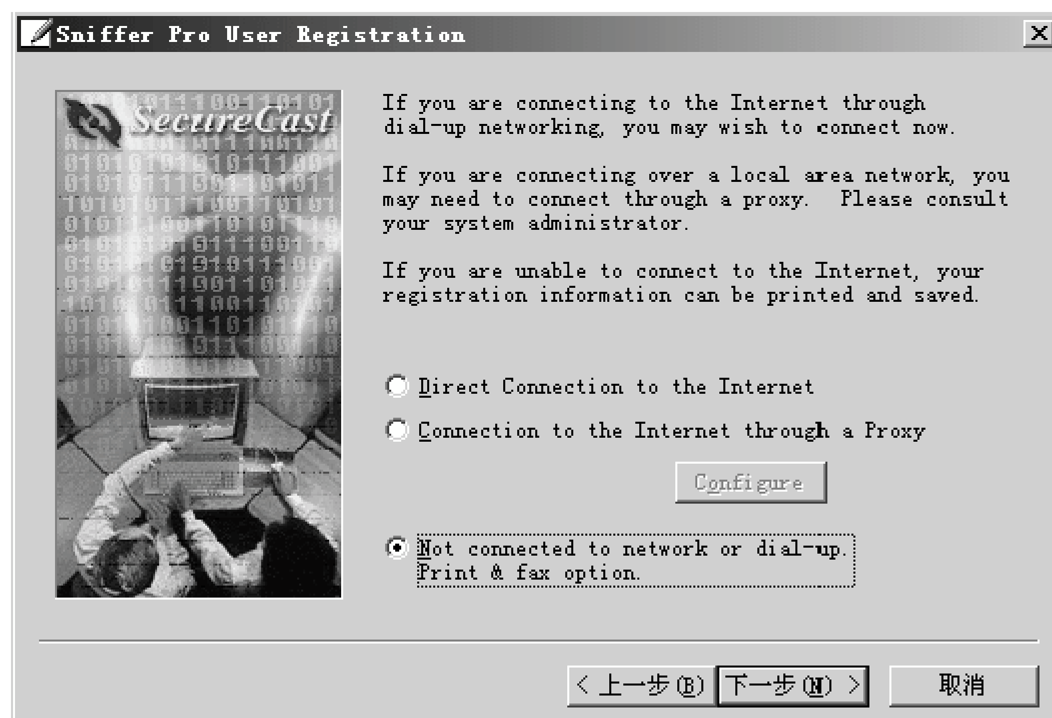


图 18-38　Sniffer Pro User Registration 对话框

11 弹出 Sniffer Pro User Registration 对话框，单击【完成】按钮，完成 Sniffer 的注册，如图 18-39 所示。

12 弹出 Setup Complete 对话框，单击 Finish 按钮，如图 18-40 所示。



图 18-39　Sniffer Pro User Registration 对话框



图 18-40　Setup Complete 对话框

13 弹出 Setup Complete 对话框，选择【Yes，I want to restart my computer now】（是的，我想现在重新启动我的计算机）选项，单击 Finish 按钮，如图 18-41 所示。

14 计算机重启之后，Sniffer Pro 安装完成。但是要想完整地显示 Sniffer Pro 操作界面，还必须安装 JDK 软件包，双击 JDK 安装文件，弹出【Java SE Development Kit 6 update 10 – 许可证】（JDK6.10 安装许可证）对话框，单击【接受】按钮，如图 18-42 所示。



图 18-41　Setup Complete 对话框

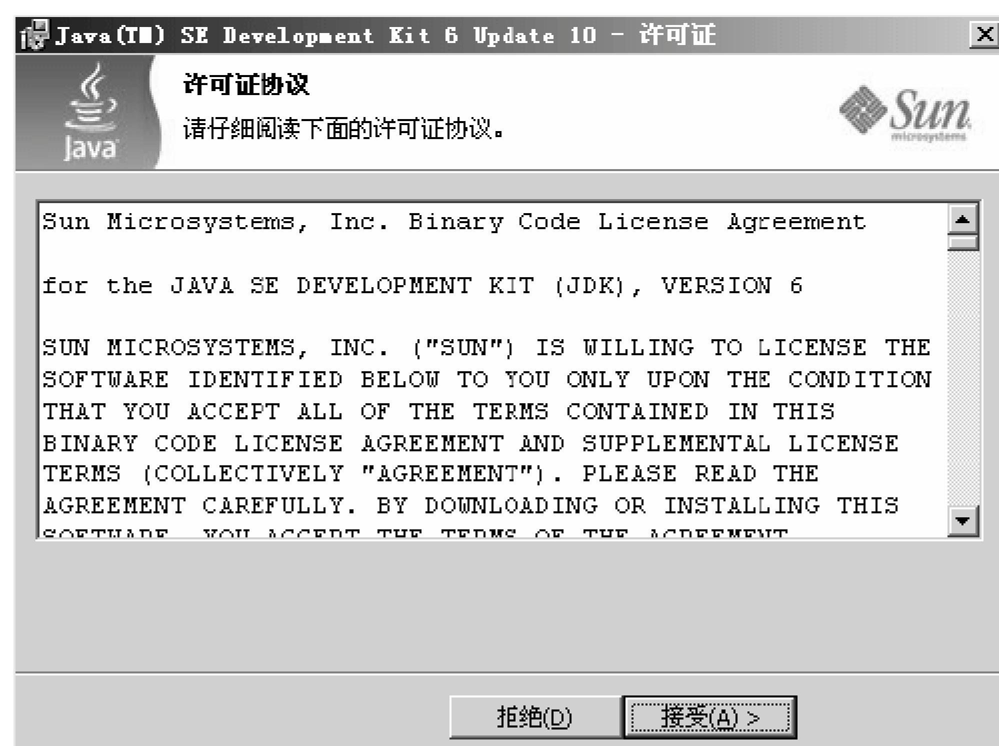


图 18-42　许可证协议对话框

15 弹出【自定义安装】对话框，单击【更改】按钮自定义 JDK 的安装路径，单击【下一步】按钮，如图 18-43 所示。

16 JDK 安装程序正在继续安装，显示安装进度，如图 18-44 所示。

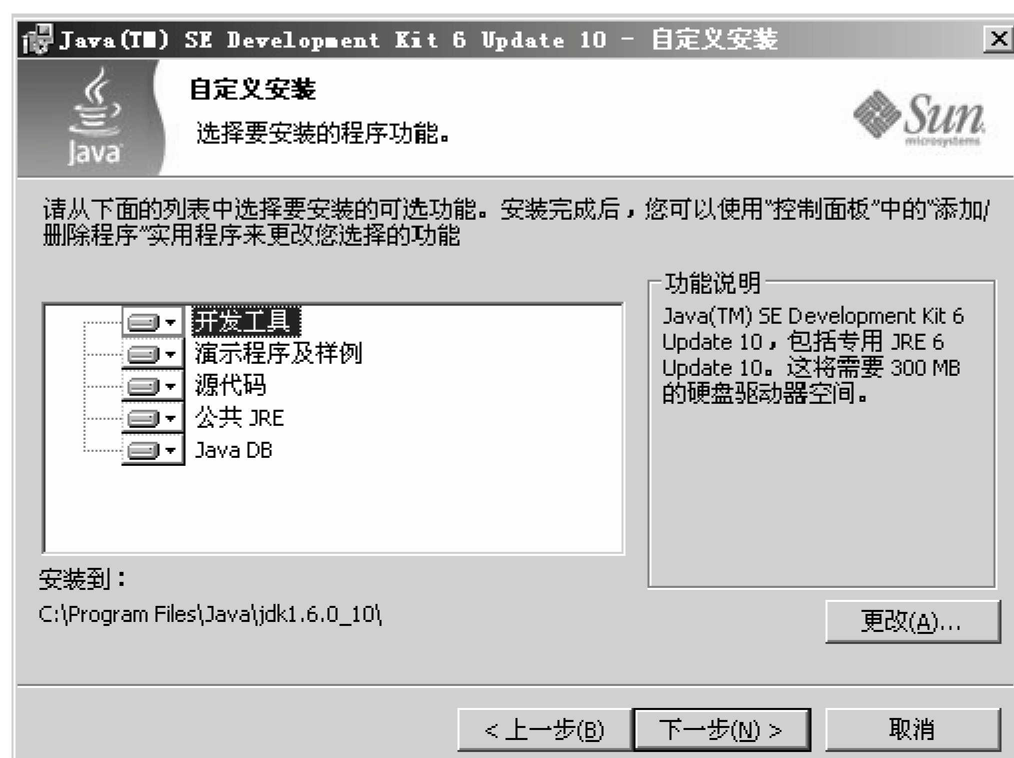


图 18-43　【自定义安装】对话框



图 18-44　JDK 功能文件复制对话框

17 弹出【目标文件夹】对话框，单击【更改】按钮自定义 Java 安装路径，单击【下一步】按钮，如图 18-45 所示。

18 JDK 安装程序正在继续安装，并显示安装进度，如图 18-46 所示。



图 18-45　【目标文件夹】对话框



图 18-46　JDK 安装进度对话框

19 JDK 安装结束，单击【完成】按钮，完成 JDK 的安装，如图 18-47 所示。



图 18-47　JDK 安装向导结束对话框

18.4.2　设置 Sniffer Pro 监控网络适配器

如果安装有 Sniffer 的服务器有两块以上的网卡，就需要设置 Sniffer Pro 的监听网卡。由于所有的局域网数据包都通过代理服务器的内网网卡连接互联网，如果想要监听内网与外网的所有通信，就需要 Sniffer Pro 监控代理服务器的内网网卡。

具体的操作步骤如下。

01 选择【开始】➢【所有程序】➢ Sniffer Pro ➢ Sniffer 命令，打开 Sniffer Pro 软件，如图 18-48 所示。

02 弹出 Settings 对话框，选择代理服务器的内网网卡也就是 Sniffer Pro 要监控的网卡，单击【确定】按钮，如图 18-49 所示。



图 18-48　sniffer 选项

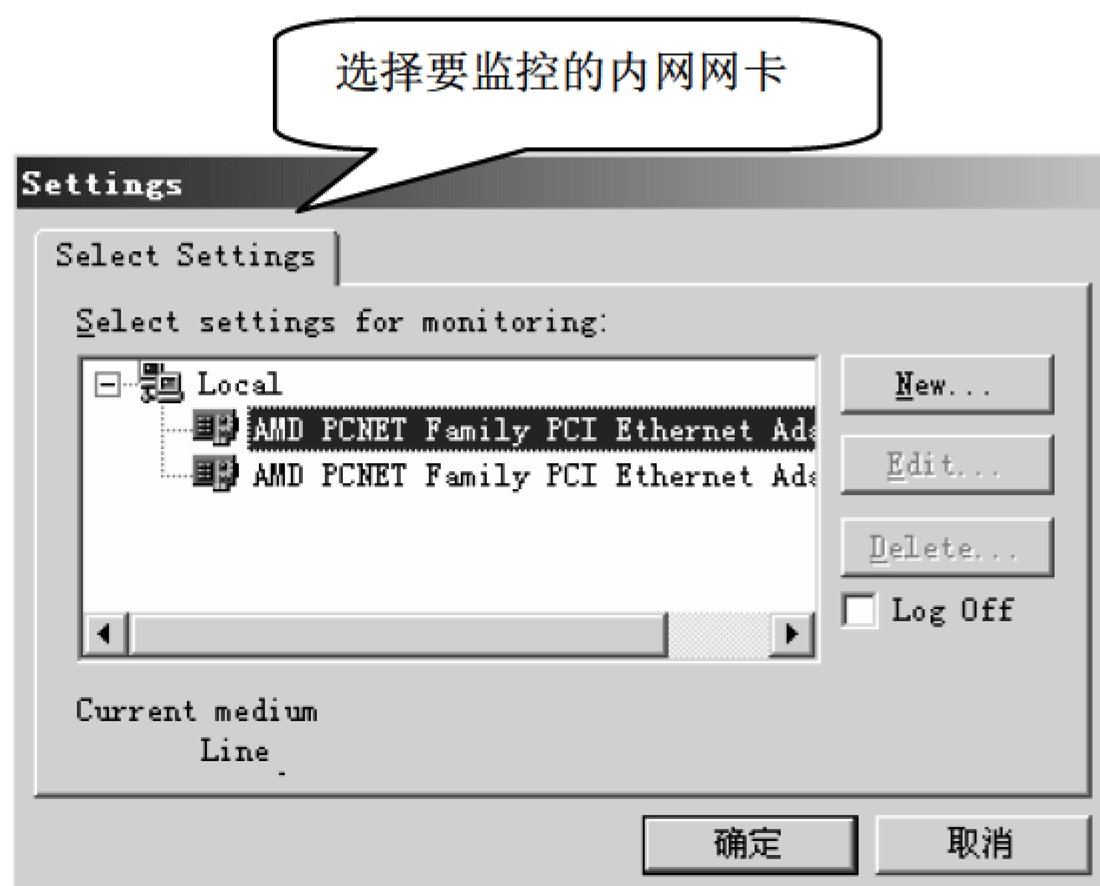


图 18-49　Settings 对话框

03 弹出 Sniffer Pro 程序的主界面，主界面由工具栏、仪表盘和流量统计三部分构成，如图 18-50 所示。



图 18-50 Sniffer Pro 程序的主界面

18.4.3 Sniffer 的监控功能

Sniffer 的主要功能是监控网络中数据包的传输。Sniffer 主要有七大监控功能，包括 Dashboard（仪表）、Host Table（主机列表）、Matrix（矩阵）、ART（应用响应时间）、Protocol Distribution（协议分类）、History Sample（历史采样）和 Global Statistics（球状统计）。合理使用这些功能可以帮助网络管理员实时查看网络中传输的数据，便于网络管理员及时发现故障并解决。

1. Dashboard

Sniffer Pro 使用各种仪表盘将捕捉到的数据包以人性化的方式显示，熟练使用 Sniffer Pro 的各种仪表盘有助于快速分析数据包并解决问题。

Sniffer Pro 仪表盘使用图形化界面，可以直观检测到网络的利用情况，具体的操作步骤如下。

01 在 Sniffer Pro 的程序主界面选择 Monitor ➢ Dashboard 命令，可以打开 Sniffer Pro 仪表盘。Sniffer Pro 的仪表盘有 Utilization%（利用率百分比）、Packets/s（每秒传输的数据包）和 Error/s（每秒产生的错误）三个表盘，如图 18-51 所示。

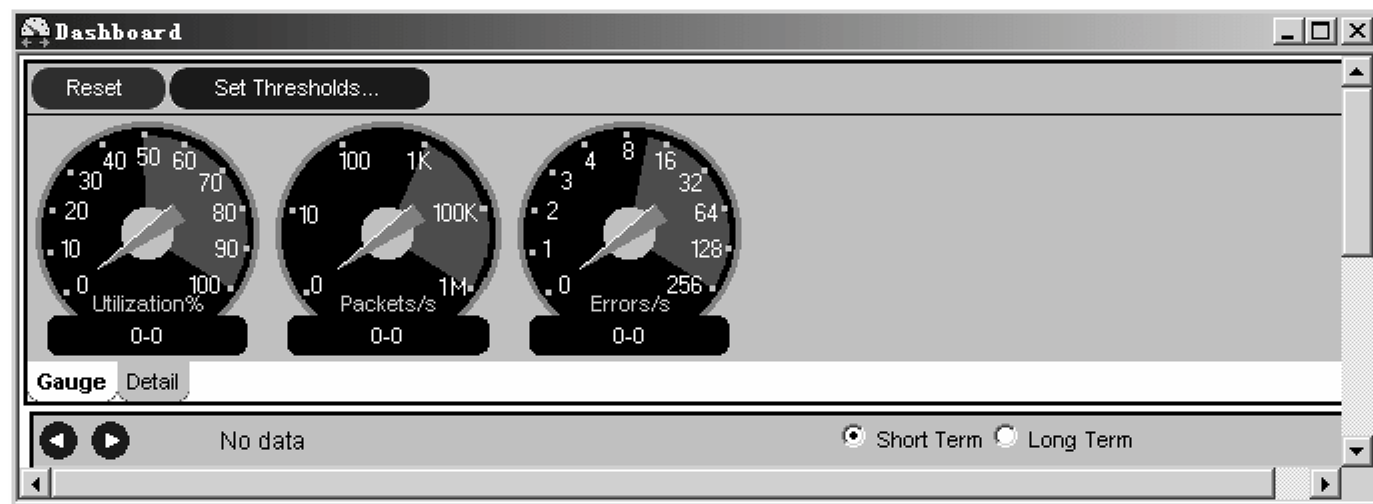


图 18-51 Sniffer Pro 仪表盘



提 示

Sniffer Pro 的三个仪表盘下面都有两个数字，前面一个数字是当前值，后面一个数字是最大值。

三个仪表盘的含义如下。

- Utilization%：表示网络带宽利用率，也就是现在网络流量所占带宽占总带宽的百分比。利用率百分比应该根据不同的网络情况来进行区分，不同的网络或者不同的网络拓扑网络带宽利用率不一样。例如，以太网的网络带宽如果能超过 40%就算很高了，但是全双工以太网中网络带宽需要达到 80%才算高。
- Packets/s：每秒钟传输的数据包数量。可以帮助管理员更详细地了解每秒钟网络中传输帧的大小。通过每秒钟传输的数据包可以分析出当前网络传输速度。若网络利用率较小但数据传输速度比较快，说明网络中传输的数据包较小。
- Error/s：每秒产生的错误数据包数。很多网络管理员一听到错误数据包数量，就认为如果每秒钟产生的错误过多就是网络出现了问题，其实并非每个错误数据包都有问题。如在以太网产生的数据包冲突也是错误数据包，这种数据包只要不是过多就不会带来问题。

02 如果想要查看数据包的详细信息，单击在 Utilization%仪表盘下面的 Detail（详细信息）标签，打开详细信息界面，在其中查看相关的详细信息。单击仪表盘上的 Set Thresholds（设置阀值）按钮，如图 18-52 所示。

03 弹出 Dashboard Properties（仪表盘内容）对话框，可以设定仪表盘的阀值，阀值就是当网络中的流量达到一定数值时，Sniffer Pro 用红色进行报警，如图 18-53 所示。

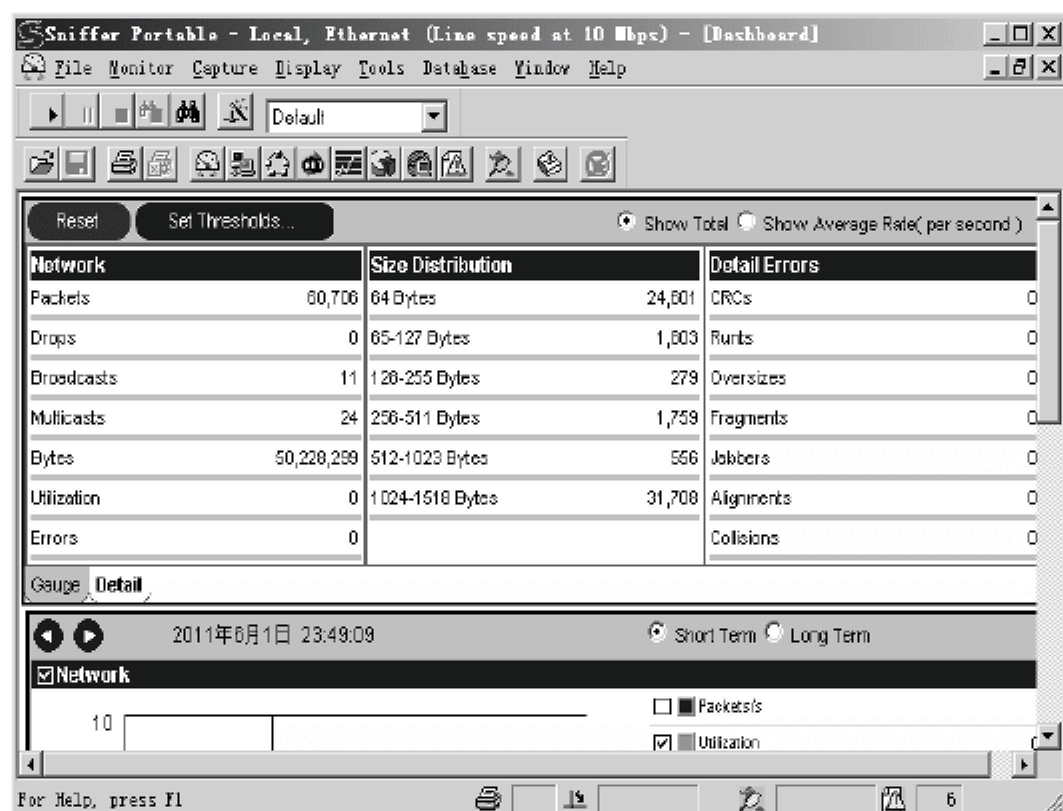


图 18-52　详细信息界面

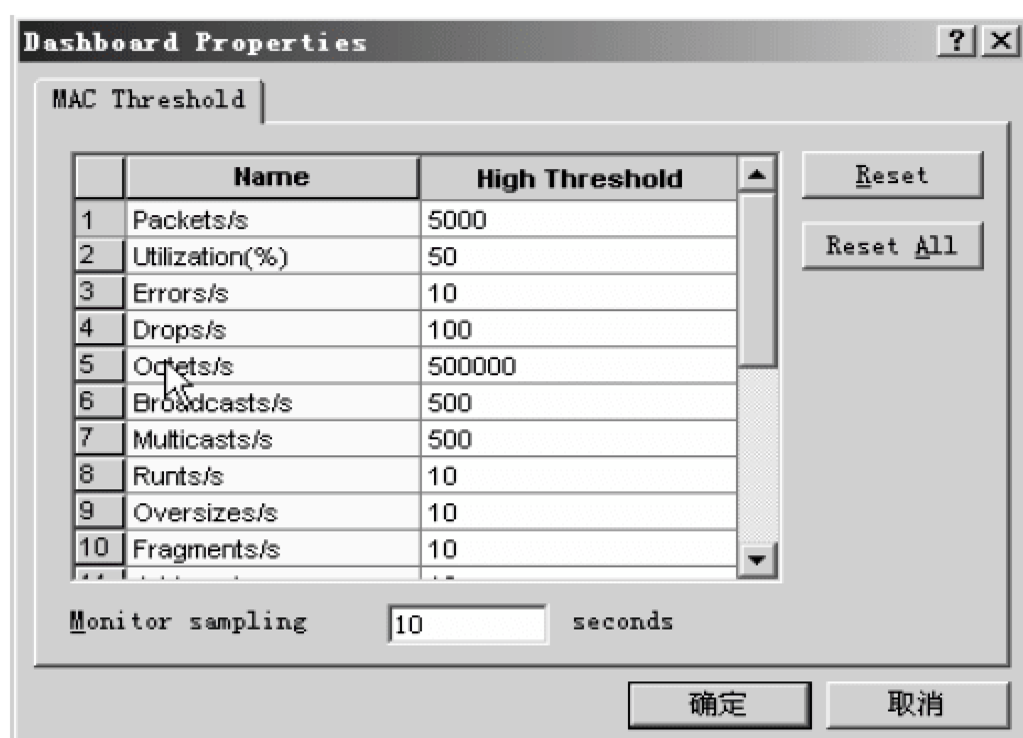


图 18-53　Dashboard Properties 对话框

2. Host Table

Host Table 以列表的形式显示了当前网络中计算机的通信信息，包含发送数据包、接收数据包和错误数据包等信息。如果一个主机在一定的时间内发送或者接收了大量的数据包，该计算机可能正在使用 BT、P2P 等下载软件。

以主机列表形式查看计算机通信信息的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面选择 Monitor ➢ Host Table 选项，打开 Host Table 窗口。该窗

口列出了当前捕捉到的网络主机通信信息，如图 18-54 所示。

Host Table: 69 stations

Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Out Errors	CRC
000AEB4B7E43	0	5	0	500	5	0	5	
000AEB4B7E46	0	2	0	311	2	0	2	
000AEB4B7E5C	[illegible]	[illegible]	0	64	1	0	1	
000AEB4BBFA3	[illegible]	[illegible]	0	439	4	0	4	
000AEB9AECB7	[illegible]	[illegible]	5,149	24,504	114	0	102	
000AEBA86F57	[illegible]	[illegible]	0	192	3	0	3	
000AEBA8AD10	0	65	0	6,671	65	0	58	
000AEBA8AD2B	0	2	0	128	2	0	2	
000AEBF7B560	0	1	0	64	1	0	1	
000AEBF7FCB8	0	4	0	256	4	0	3	
000AEBF85259	0	1	0	64	1	0	1	
000B7412E01E	0	19	0	1,216	19	0	17	
000C29878EC8	16	26	11,027	5,149	1	0	23	
0014783046C7	0	5	0	599	5	0	5	
001478319C08	0	1	0	64	1	0	1	
001478404FAC	0	5	0	680	5	0	3	
001478410648	0	2	0	128	2	0	2	
0014784257BA	0	5	0	525	5	0	5	
00147842972C	0	52	0	3,704	52	0	49	
00192188C22F	0	2	0	128	2	0	2	
00192188D6E4	0	2	0	128	2	0	1	
00192189CCD7	0	3	0	555	3	0	2	
00192189D7CE	0	4	0	436	4	0	4	
00192189D94D	0	1	0	64	1	0	1	
001921B6D400	1	326	64	31,112	326	0	259	
001FC62BBCC0	0	33	0	2,979	33	0	28	

MAC IP IPX

图 18-54 Host Table 窗口

显示的信息项目内容解释如下。

- Hw Addr：默认情况下主机列表以 MAC 地址的形式表示通信主机。
- In Pkts：此主机接收的数据包。
- Out Pkts：此主机发送的数据包。
- In Byts：此主机接收的字节数。
- Out Bytes：此主机发送的字节数。
- Broadcast：此主机广播的数据包。
- Out Errors：此主机传出的错误数据包。

02 单击 Host Table 窗口左下方的 IP 标签，则 Sniffer Pro 将以 IP 地址的形式标示捕捉到的网络主机，如图 18-55 所示。

Host Table: 42 stations

IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Update Time
0.0.0.0	0	4	0	1,384	4	0	2011-06-02 16:18:34.993
58.251.61.139	22	38	7,204	47,468	0	0	2011-06-02 16:32:29.652
60.28.14.147	9	28	576	10,169	0	0	2011-06-02 16:32:29.651
125.39.127.25	11	22	4,274	17,134	0	0	2011-06-02 16:32:22.478
169.254.21.31	0	2	0	293	0	1	2011-06-02 16:16:12.88
169.254.255.255	1	0	114	0	0	0	2011-06-02 16:15:59.21
172.16.1.254	0	68	0	26,197	0	68	2011-06-02 16:32:30.649
172.16.2.1	55	22	40,385	6,090	0	0	2011-06-02 16:32:29.651
172.16.2.44	0	3	0	439	0	0	2011-06-02 16:29:15.401
172.16.255.255	3	0	439	0	0	0	2011-06-02 16:29:15.401
192.168.1.11	0	1	0	96	0	0	2011-06-02 16:27:13.982
192.168.1.20	0	2	0	488	0	0	2011-06-02 16:18:55.118
192.168.1.22	0	1	0	220	0	0	2011-06-02 16:20:54.231
192.168.1.37	0	1	0	235	0	0	2011-06-02 16:17:49.467
192.168.1.39	0	2	0	470	0	0	2011-06-02 16:23:18.421
192.168.1.54	0	1	0	255	0	0	2011-06-02 16:23:13.825
192.168.1.55	0	1	0	259	0	0	2011-06-02 16:22:30.557
192.168.1.61	[illegible]	[illegible]	0	4,896	38	0	2011-06-02 16:32:26.587
192.168.1.68	[illegible]	[illegible]	[illegible]	14,849	0	0	2011-06-02 16:32:34.169
192.168.1.75	[illegible]	[illegible]	[illegible]	1,502	0	10	2011-06-02 16:32:06.813
192.168.1.79	[illegible]	[illegible]	[illegible]	735	4	0	2011-06-02 16:32:27.265
192.168.1.80	[illegible]	[illegible]	[illegible]	244	0	0	2011-06-02 16:21:03.514
192.168.1.144	[illegible]	[illegible]	[illegible]	96	0	0	2011-06-02 16:17:28.232
192.168.1.147	[illegible]	[illegible]	[illegible]	976	0	0	2011-06-02 16:27:19.153
192.168.1.151	0	3	0	560	0	0	2011-06-02 16:29:23.877
192.168.1.166	0	1	0	244	0	0	2011-06-02 16:21:03.722

MAC IP PX

图 18-55 以 IP 地址的形式表示捕捉到的网络主机

3. Matrix

Matrix 以矩阵的形式来显示当前的网络通信信息，通过矩阵可以清晰看到网络中主机正在与哪些主机进行通信，当某个主机不停地在和大量的主机同时进行通信时，怀疑该主机是否中了蠕虫病毒或者正在使用 BT 等 P2P 下载软件。

以矩阵方式查看网络通信信息的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面选择 Monitor ➢ Matrix 选项，打开 Matrix 窗口。该窗口列出了当前捕捉到的网络主机通信信息，默认情况下在矩阵中以 MAC 地址的形式来表示网络中的主机，如图 18-56 所示。

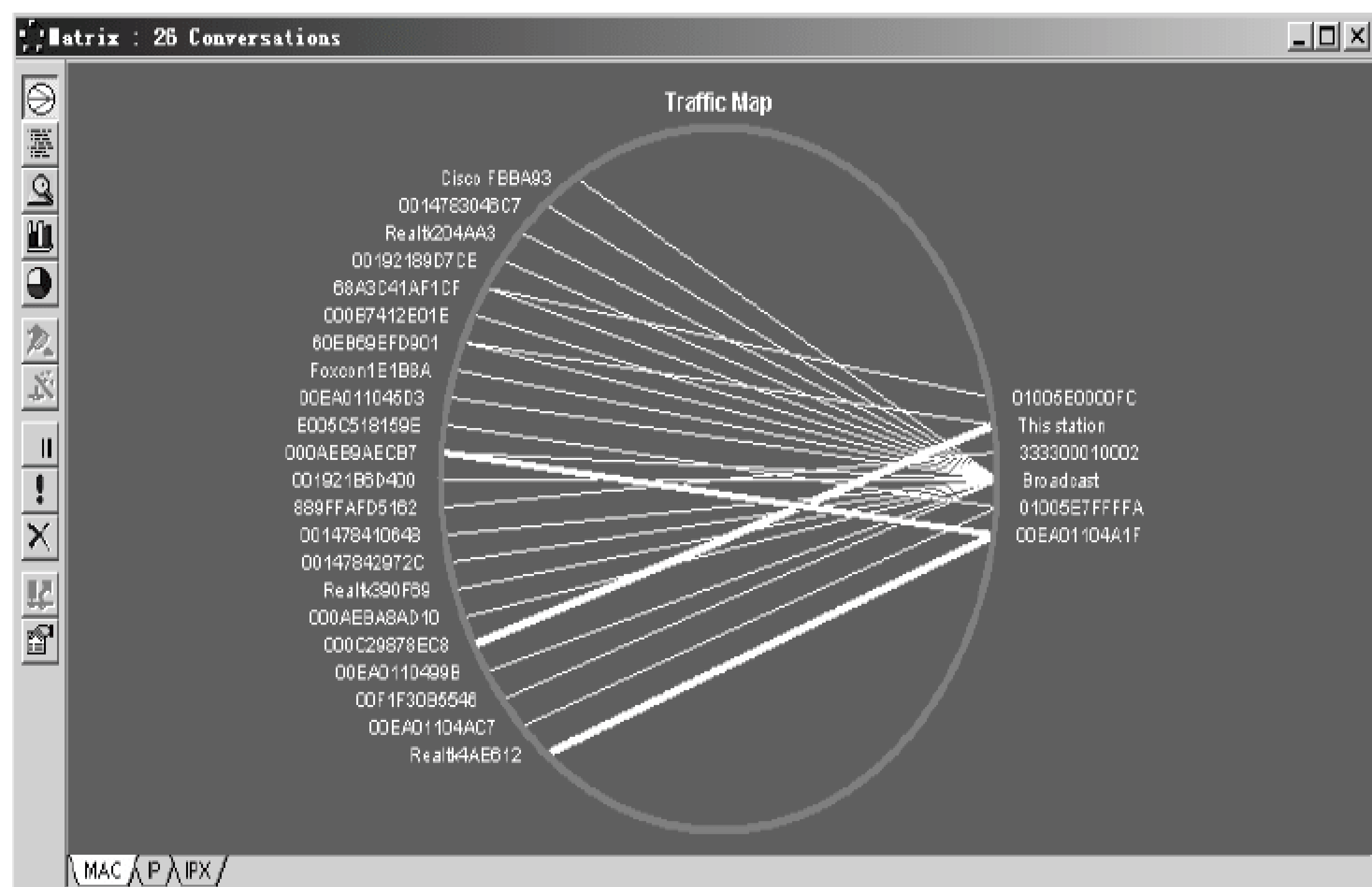


图 18-56 Matrix 窗口

图 18-58 中线条的颜色表示相应的通信状态如下。

（1）绿色线条状态为正在通信中。

（2）暗蓝色线条状态为通信中断。

（3）线条的粗细与流量的大小成正比。

（4）如果将鼠标移动至线条处，程序显示出流量双方位置、通信流量的大小并自动计算流量占当前网络的百分比。

02 单击 Matrix 窗口左下方的 IP 标签，则 Sniffer Pro 将以 IP 地址的形式标示捕捉到的网络主机，如图 18-57 所示。

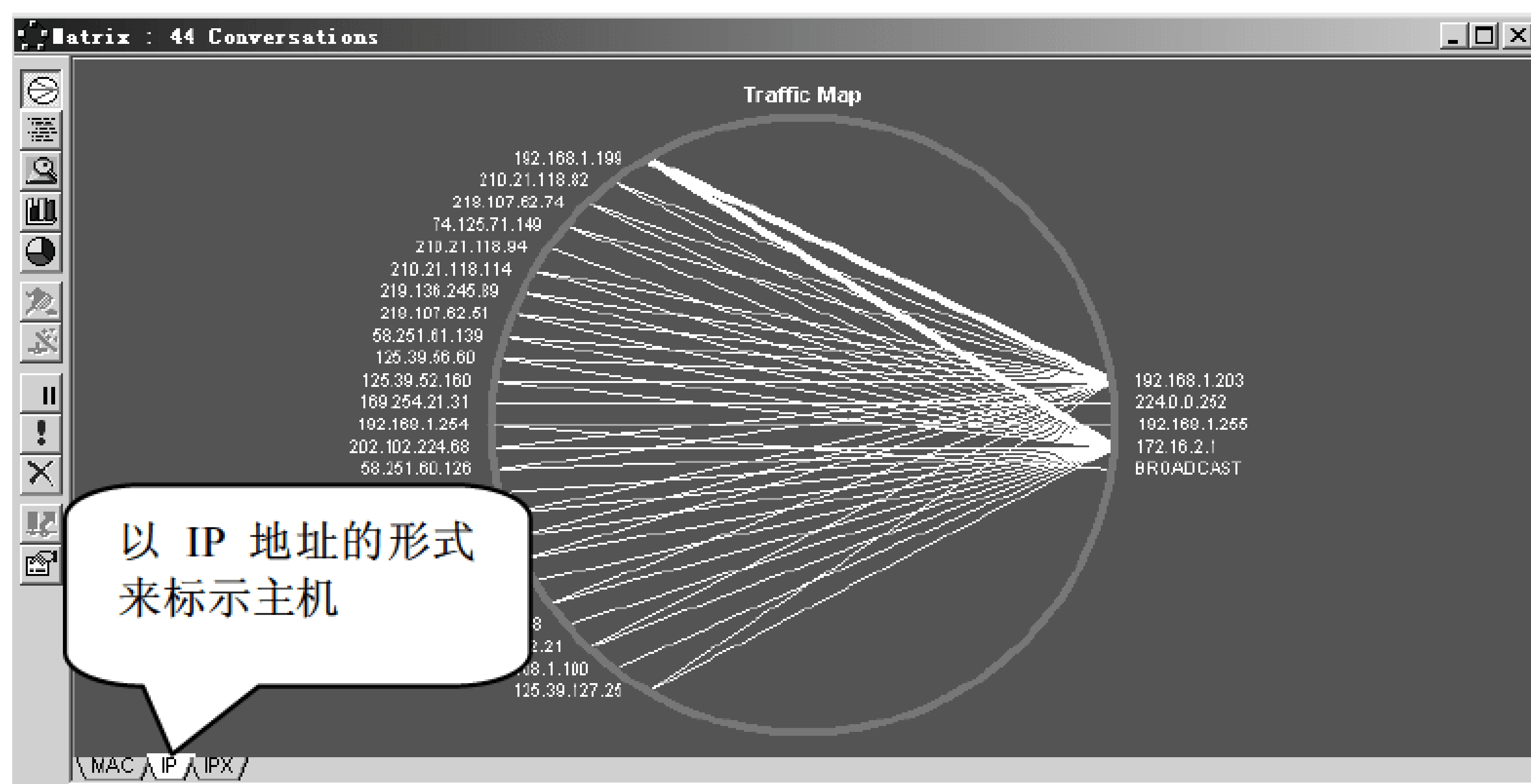


图 18-57　以 IP 地址的形式标示捕捉到的网络主机

4. ART

ART 主要显示网络中主机的上网行为，通过 ART 可以看出网络主机的 HTTP 连接情况，可以直观看到网络用户正在浏览什么网站。

在 Sniffer Pro 的操作界面选择 Monitor ➢ Application Response Time 命令，打开 Application Response Time 窗口，这里列出了网络主机正在使用 HTTP 协议和网络中的哪些主机进行通信，如图 18-58 所示。

Application Response Time (milliseconds) - HTTP: 14 Entries

Server Address	Client Address	AvgRsp	90%Rsp	MinRsp	MaxRsp	TotRsp	0-25	26-50	51-100	101-200	201-400	401-800	8(
116.255.136.105	howin-1f80af4ed	125	222	2	273	7	2	0	0	4	1	0	0
116.255.136.105	bogon	125	222	3	273	7	2	0	0	4	1	0	0
123.196.117.6	howin-1f80af4ed	68	99	3	217	11	2	1	7	0	1	0	0
123.196.117.6	bogon	69	99	3	217	11	2	1	7	0	1	0	0
216.218.207.147	howin-1f80af4ed	366	518	184	548	2	0	0	0	1	0	1	0
216.218.207.147	bogon	366	518	185	548	2	0	0	0	1	0	1	0
hx-in-f157.1e100.n	howin-1f80af4ed	97	173	3	191	2	1	0	0	1	0	0	0
hx-in-f157.1e100.n	bogon	98	173	4	192	2	1	0	0	1	0	0	0
hx-in-f166.1e100.n	howin-1f80af4ed	63	118	4	122	2	1	0	0	1	0	0	0
hx-in-f166.1e100.n	bogon	63	118	4	122	2	1	0	0	1	0	0	0
reverse.gdsz.cncn	howin-1f80af4ed	71	81	38	87	3	0	1	2	0	0	0	0
reverse.gdsz.cncn	bogon	71	82	39	87	3	0	1	2	0	0	0	0
60.28.14.147	howin-1f80af4ed	47	55	37	57	3	0	2	1	0	0	0	0
60.28.14.147	bogon	48	55	38	57	3	0	2	1	0	0	0	0

HTTP

图 18-58　Application Response Time 窗口

5. Protocol Distribution

Protocol Distribution 主要显示了网络中不同协议的使用情况，查看协议分类的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面选择 Monitor➢Protocol Distribution 命令，打开 Protocol Distribution 窗口，用不同颜色显示了当前网络中不同协议的使用情况，如图 18-59 所示。

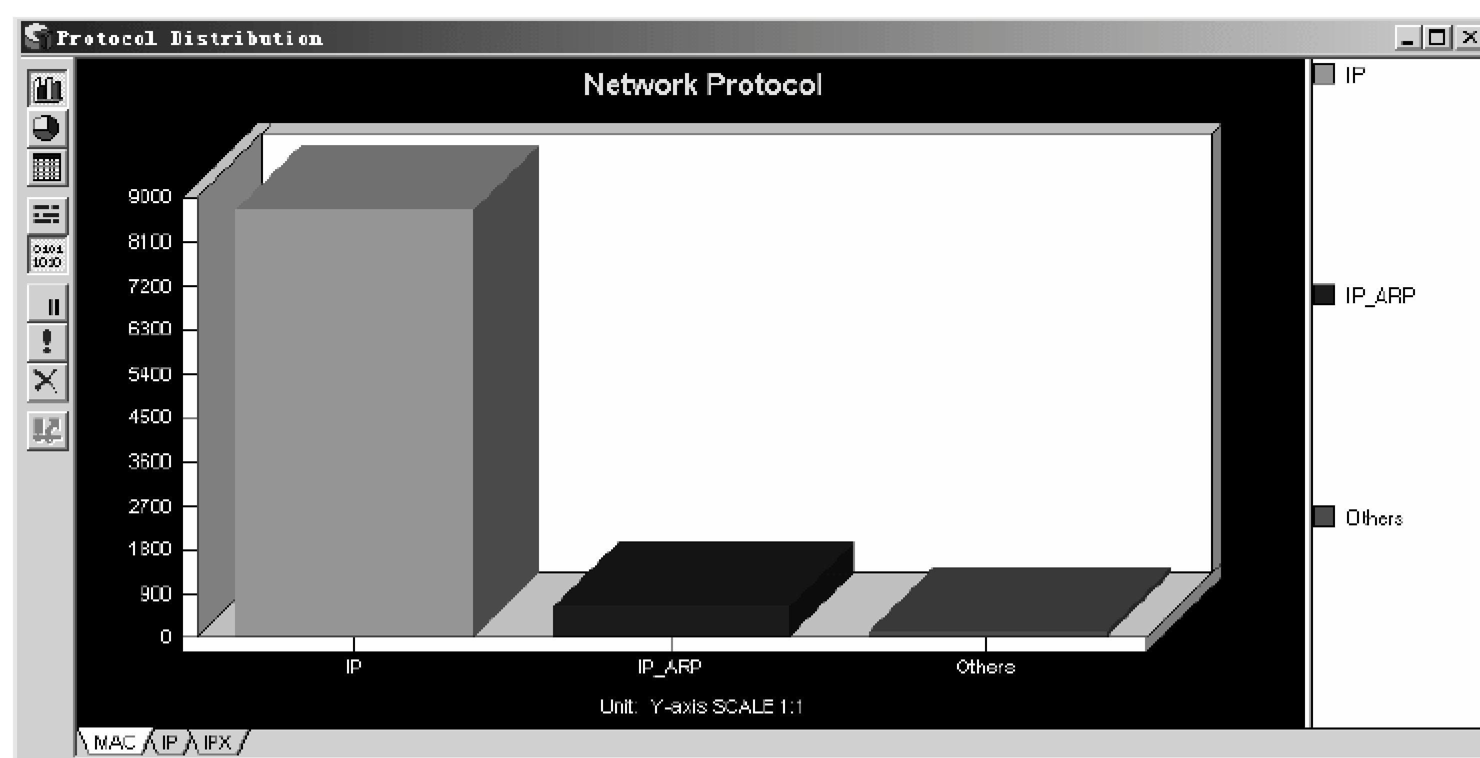


图 18-59　Protocol Distribution 窗口

02 单击工具栏左侧◕图标，将以饼形的形式来显示不同协议的使用情况，如图 18-60 所示。

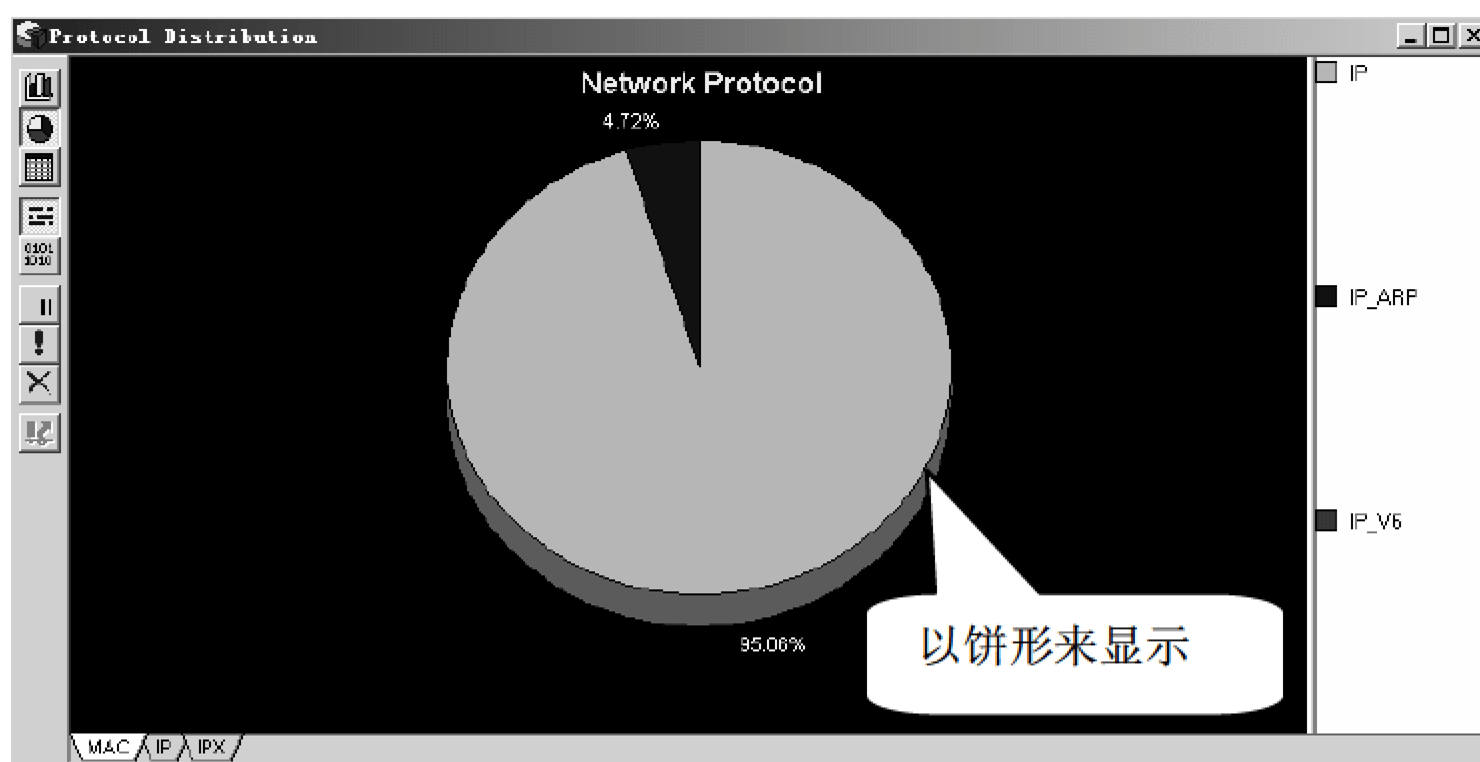


图 18-60　以饼形的形式来显示不同协议的使用情况

03 单击工具栏左侧▦图标，将以表格的形式来显示不同协议的使用情况，如图 18-61 所示。

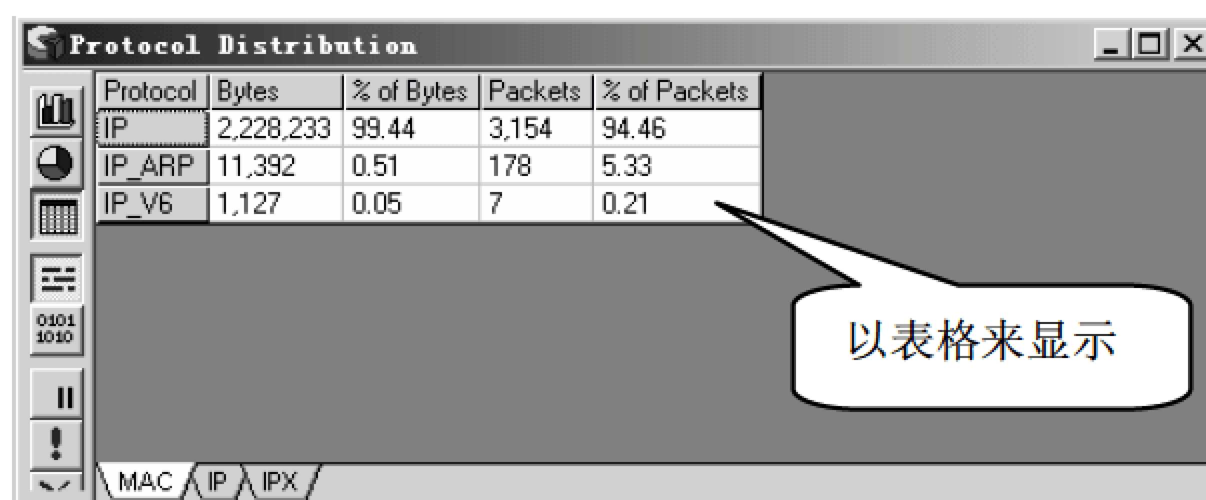


图 18-61　以表格的形式来显示不同协议的使用情况

6. History Sample

History Sample 可以捕捉到一段时间内各个阶段的网络利用情况。

在 Sniffer Pro 的操作界面中选择 Monitor ➢ History Sample 命令，打开 History Sample 窗口，如图 18-62 所示。

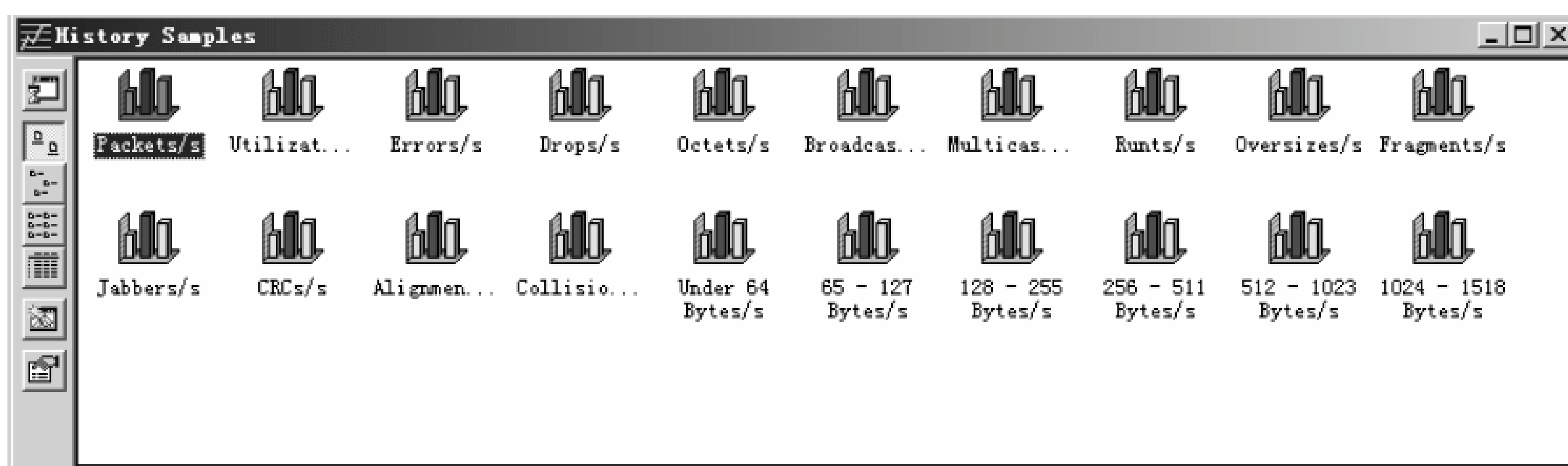


图 18-62　History Sample 窗口

如果想看网络中这一时段每秒钟传输的数据包，双击图标，弹出 Packets/s 窗口。在 Packets/s 窗口下方的时间表明捕捉的是什么时间段的数据包，History Sample 功能每隔 15 秒捕捉一次。管理员可以将这个记录进行保存，以便日后分析网络时使用，如图 18-63 所示。

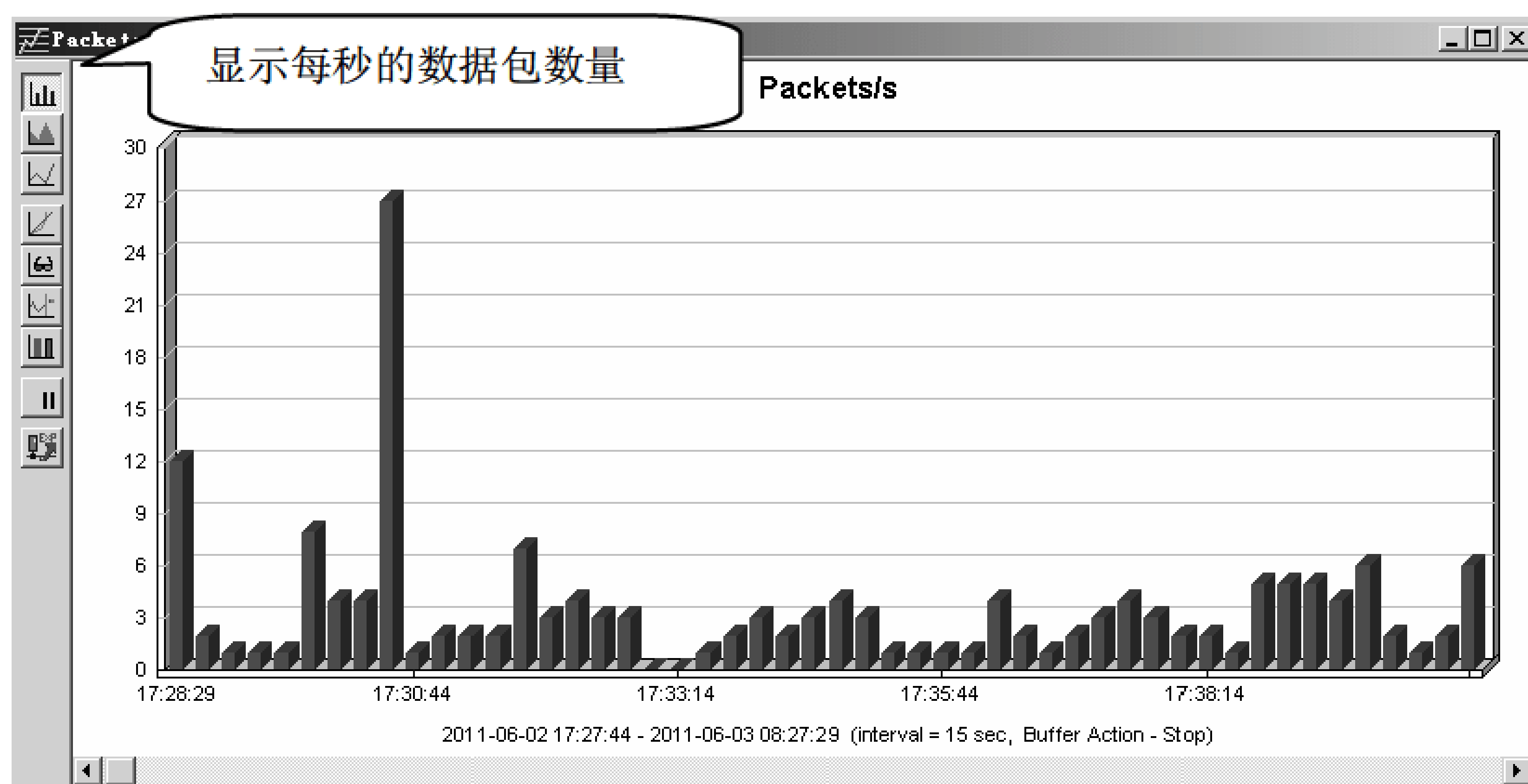


图 18-63　Packets/s 窗口

7. Global Statistics

Global Statistics 用来显示网络中传输的数据包大小分布。

在 Sniffer Pro 的操作界面中选择 Monitor ➢ Global Statistics 命令，打开 Global Statistics 窗口。在其中可以查看球状统计信息，如图 18-64 所示。

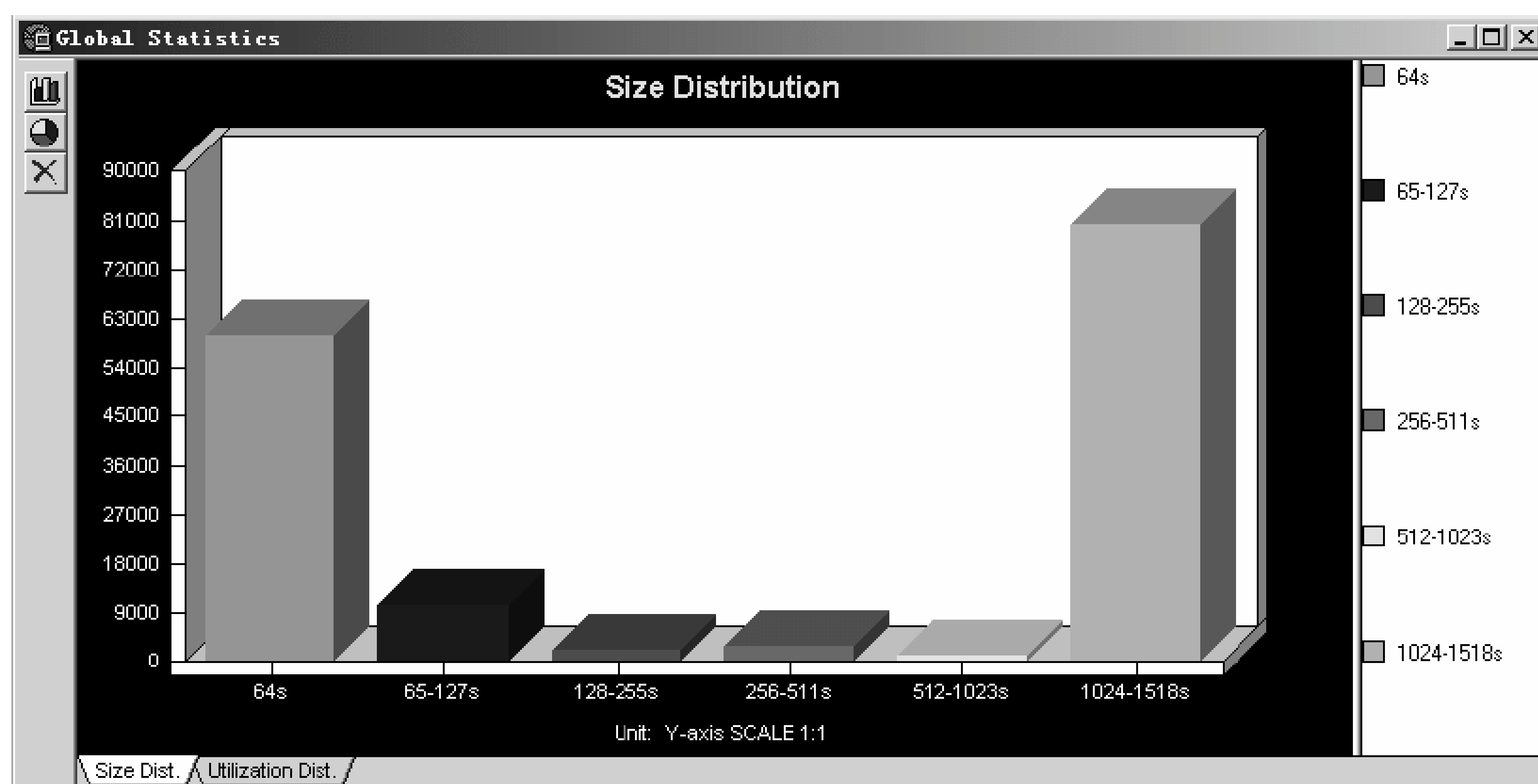


图 18-64　Global Statistics 窗口

18.4.4 捕捉数据包

默认情况下，Sniffer Pro 会监听所有的数据包，在实际的数据包捕获过程中，有些数据是无关紧要的，如特定主机的数据包、符合某种网络协议的数据包等。这时就需要设置捕捉数据包的过滤条件，这样 Sniffer 只捕捉与条件相关的数据包，可以大大节省分析数据包的时间。

1. 设置 IP 过滤规则

通过添加一个过滤器，使得 Sniffer Pro 只捕捉特定 IP 地址段的数据包，具体操作步骤如下。

01 在 Sniffer Pro 的操作界面中选择 Capture（捕获）➢ Define Filter（定义过滤器）命令，弹出 Define Filter – Capture（定义捕获过滤器）对话框，单击 Profiles（配置文件）按钮，如图 18-65 所示。

02 弹出 Capture Profiles（捕捉配置文件）对话框，单击 New 按钮，如图 18-66 所示。

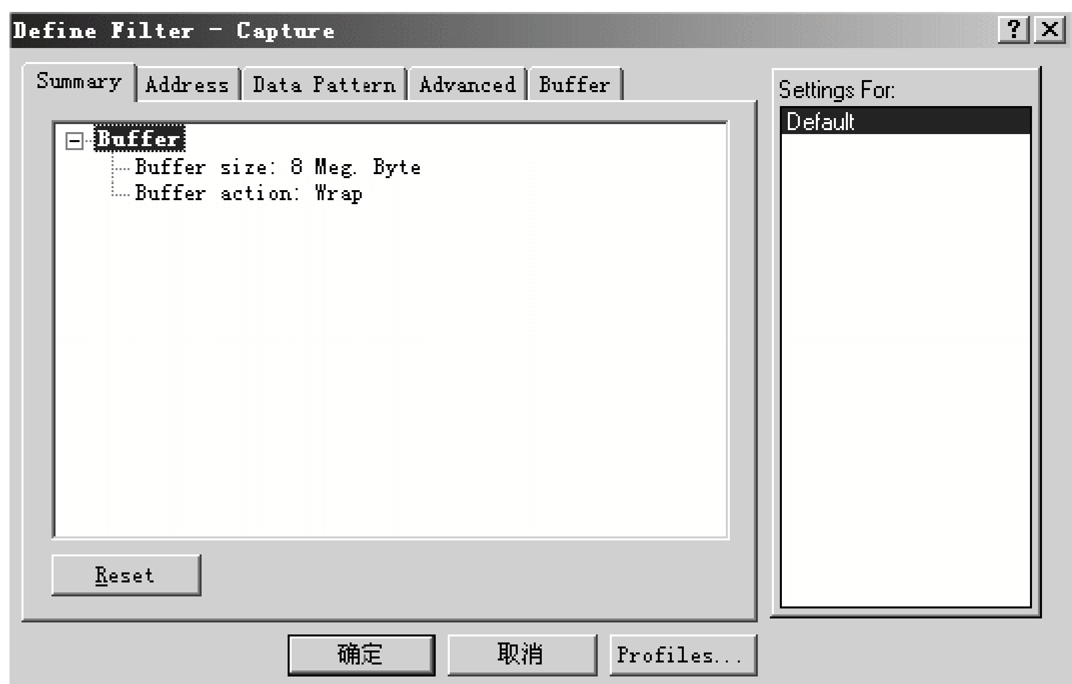


图 18-65　Define Filter – Capture 对话框

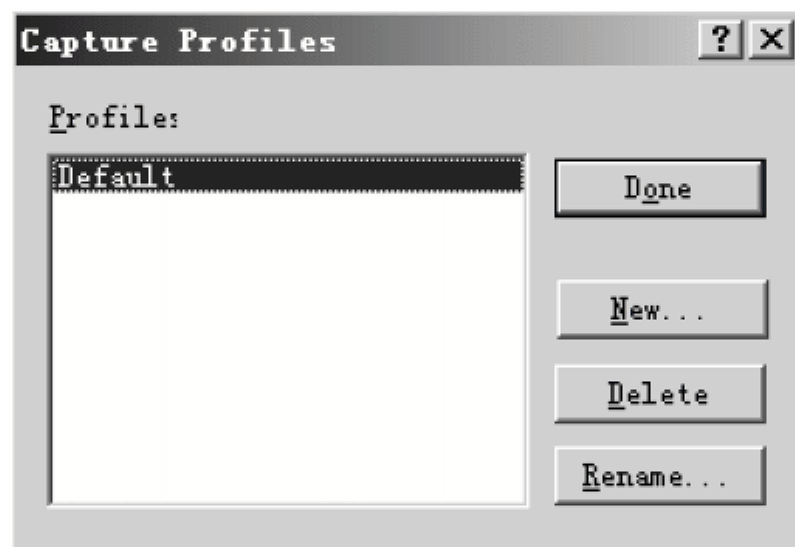


图 18-66　Capture Profiles 对话框

03 弹出 New Capture Profile（新的捕捉配置文件）对话框，在 New Profile Name（新的配置文件名字）文本框中输入过滤器的名称，单击 OK 按钮，一个新的过滤器创建完成，如图 18-67 所示。

04 返回至 Capture Profiles（捕捉配置文件）对话框，单击 Done 按钮，如图 18-68 所示。

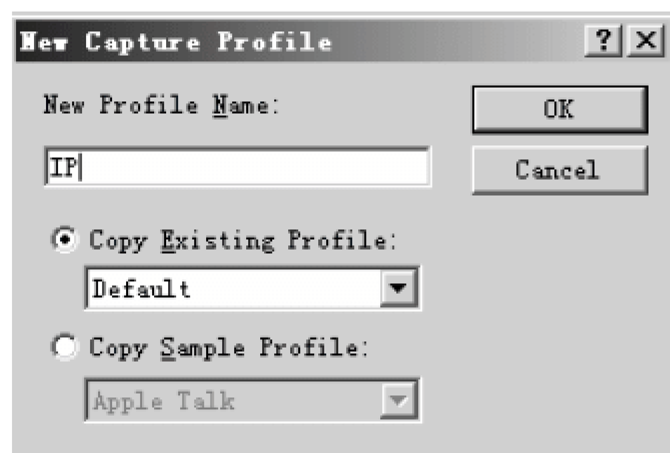


图 18-67　New Capture Profile 对话框

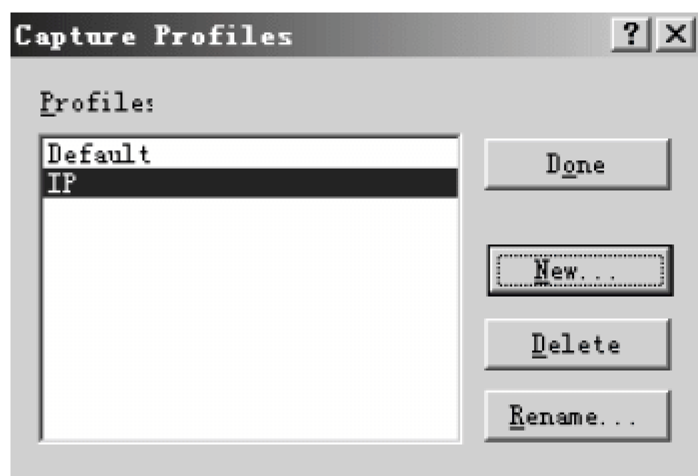


图 18-68　Capture Profiles 对话框

05 返回 Define Filter – Capture 对话框，选择 Address 选项卡，在 Address 下拉列表中选择 IP 选项，如图 18-69 所示。

06 在 Station 1（起始地址）和 Station 2（结束地址）文本框中分别输入要捕捉的 IP 地址范围，本实例输入 172.16.4.1 至 172.16.4.3，单击【确定】按钮，则一个新的 IP 过滤器创建完成，如图 18-70 所示。

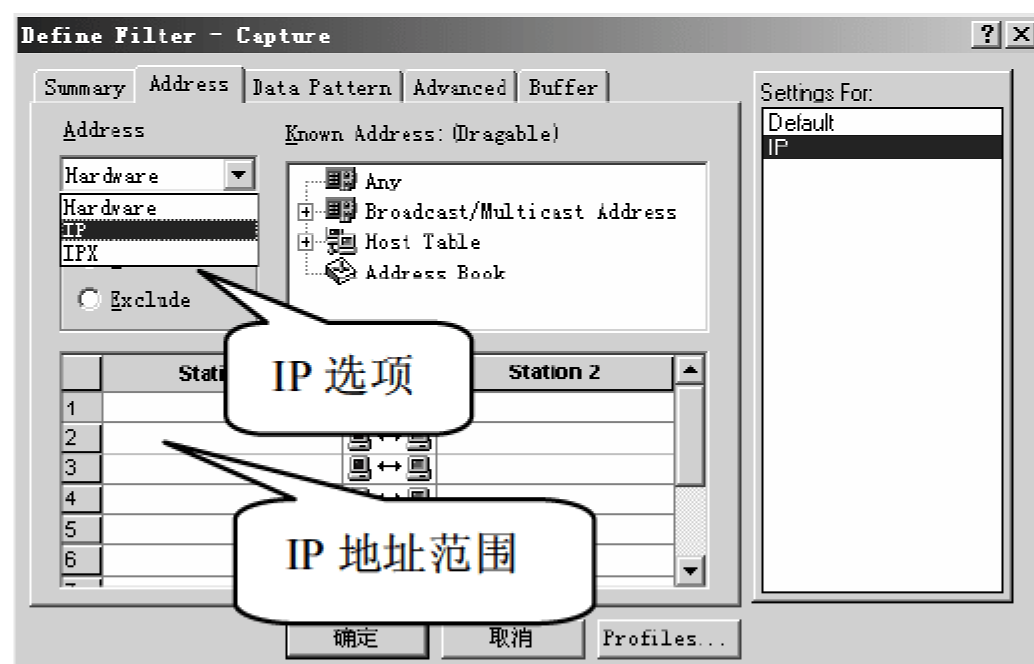


图 18-69　Address 选项卡

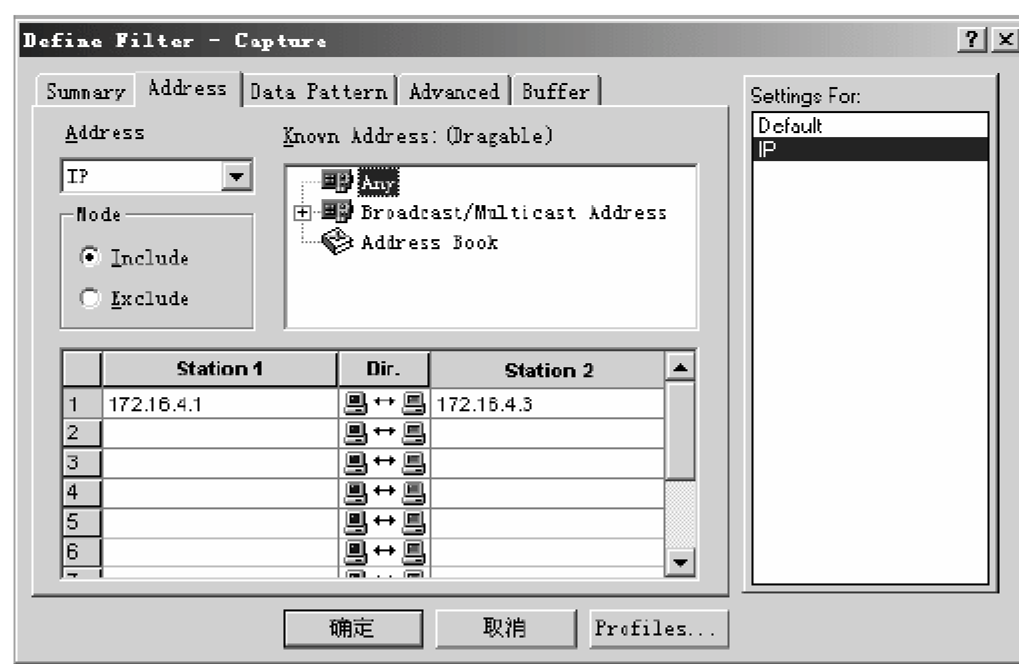


图 18-70　设定捕捉 IP 地址范围

2. 设置协议过滤规则

网络通信过程中都需要用到各种各样的网络协议，在 Snffer Pro 中可以设置在监听数据的时候，只监听某个协议或者某些协议的通信信息。

设置过滤器过滤与特定通信协议相关的数据包，具体操作步骤如下。

01 在 Sniffer Pro 的操作界面中选择 Capture➢ Define Filter 命令，弹出 Define Filter – Capture 对话框，单击 Profiles 按钮，如图 18-71 所示。

02 弹出 Capture Profiles 对话框，单击 New 按钮，如图 18-72 所示。

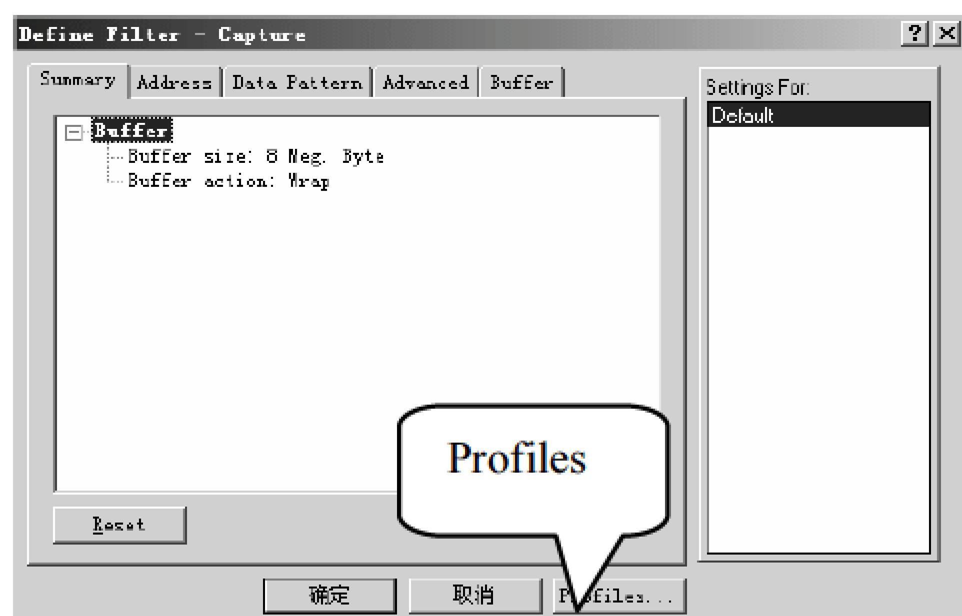


图 18-71　Define Filter – Capture 对话框

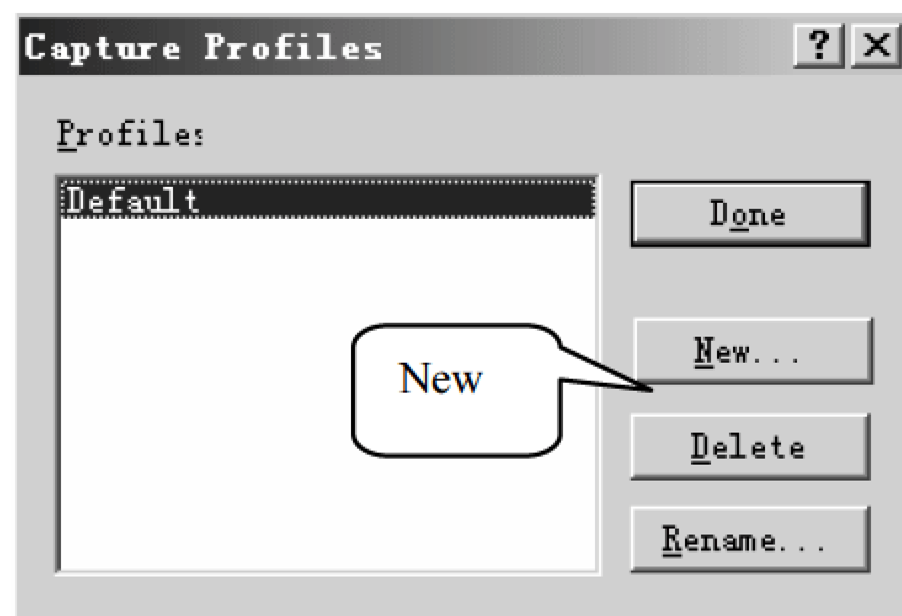


图 18-72　Capture Profiles 对话框

03 弹出 New Capture Profile（新的捕捉配置文件）对话框，在 New Profile Name（新的配置文件名字）文本框中输入过滤器的名字 protocol，单击 OK 按钮，一个新的过滤器创建完成，如图 18-73 所示。

04 返回至 Capture Profiles 对话框，单击 Done 按钮，如图 18-74 所示。

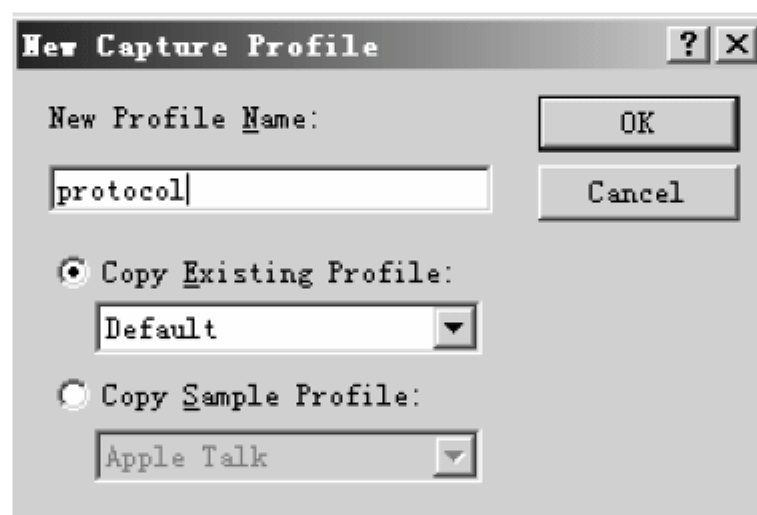


图 18-73　New Capture Profile 对话框

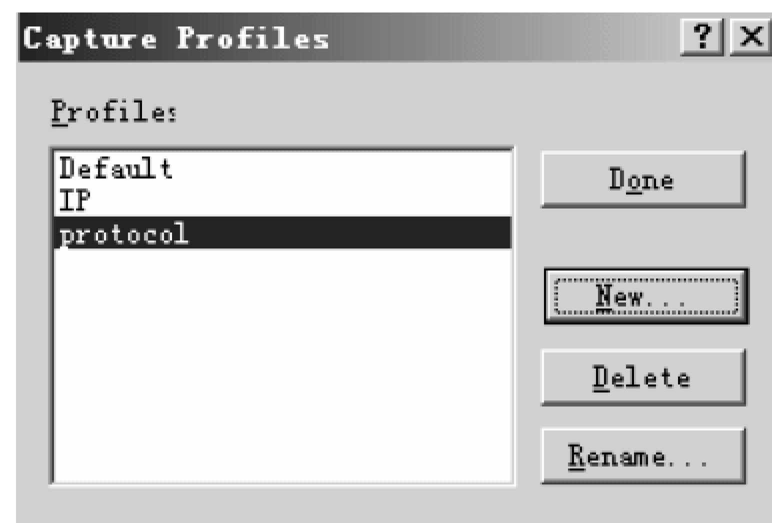


图 18-74　Capture Profiles 对话框

05 返回 Define Filter – Capture 对话框，选择 Advanced 选项卡，选择 IP ➢ TCP ➢ FTP 选项，单击【确定】按钮，一个新的网络协议过滤器创建完成，如图 18-75 所示。



图 18-75 Advanced 选项卡

默认情况下，Sniffer Pro 会捕捉所有经过 Sniffer 监听网卡的数据包，网络管理员可以对这些数据进行分析，从而发现网络存在的问题。

3. 选择合适的过滤器

在 Sniffer Pro 的操作界面中选择 Capture ➢ Define Filter 命令，弹出 Define Filter – Capture 对话框，在 Settings For（设置）列表框中选择要使用的过滤器 Default，单击【确定】按钮，如图 18-76 所示。

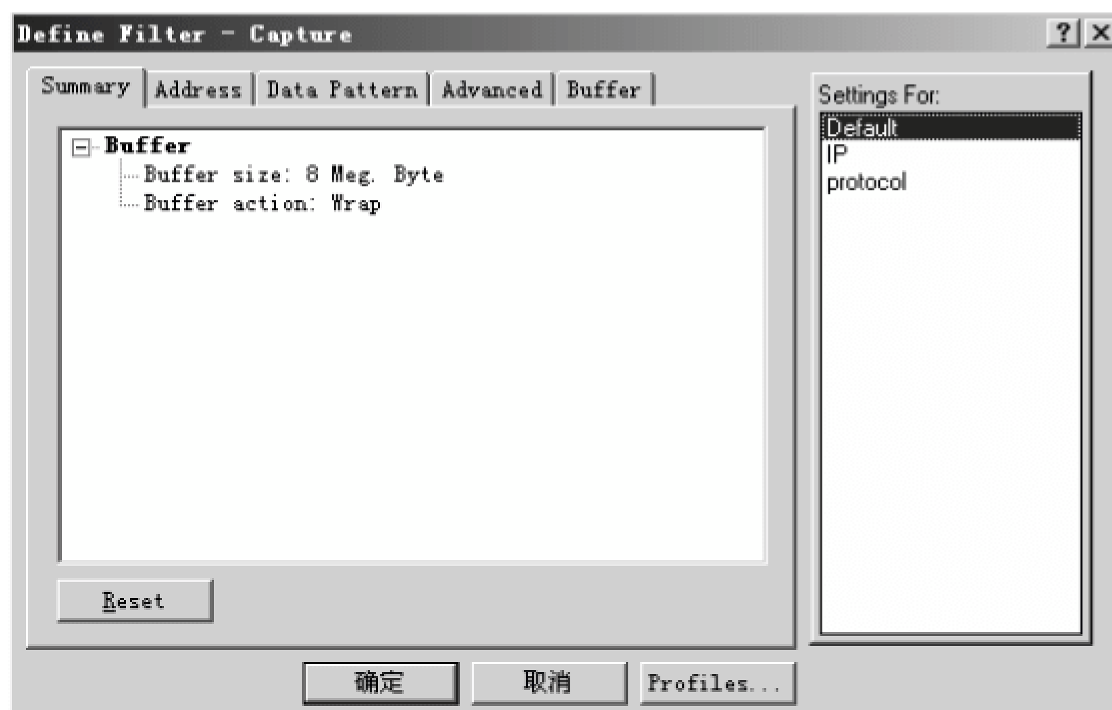


图 18-76 选择要使用的过滤器

4. 捕捉数据包

捕捉数据包的具体操作步骤如下。

01 选择 Capture ➢ start 命令，或者单击工具栏上的▶按钮开始数据包的捕捉，弹出 Expert（专家）窗口，如图 18-77 所示。

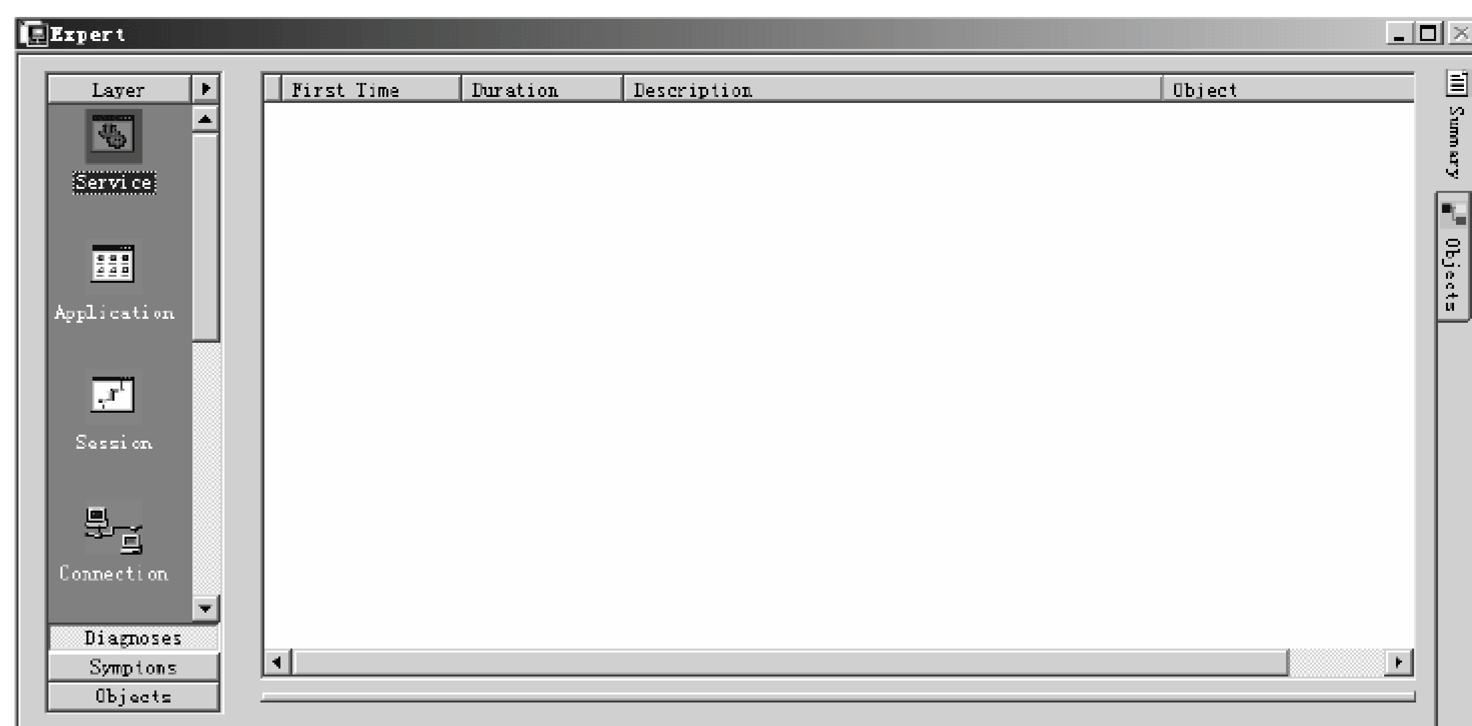


图 18-77 Expert 窗口

02 当数据包捕捉完毕后，选择 Capture ➢ stop and display 命令，或者单击工具栏上的按钮，弹出【Snif2：Expert，105 Unknown Frames】（105 个未知的帧）窗口，如图 18-78 所示。

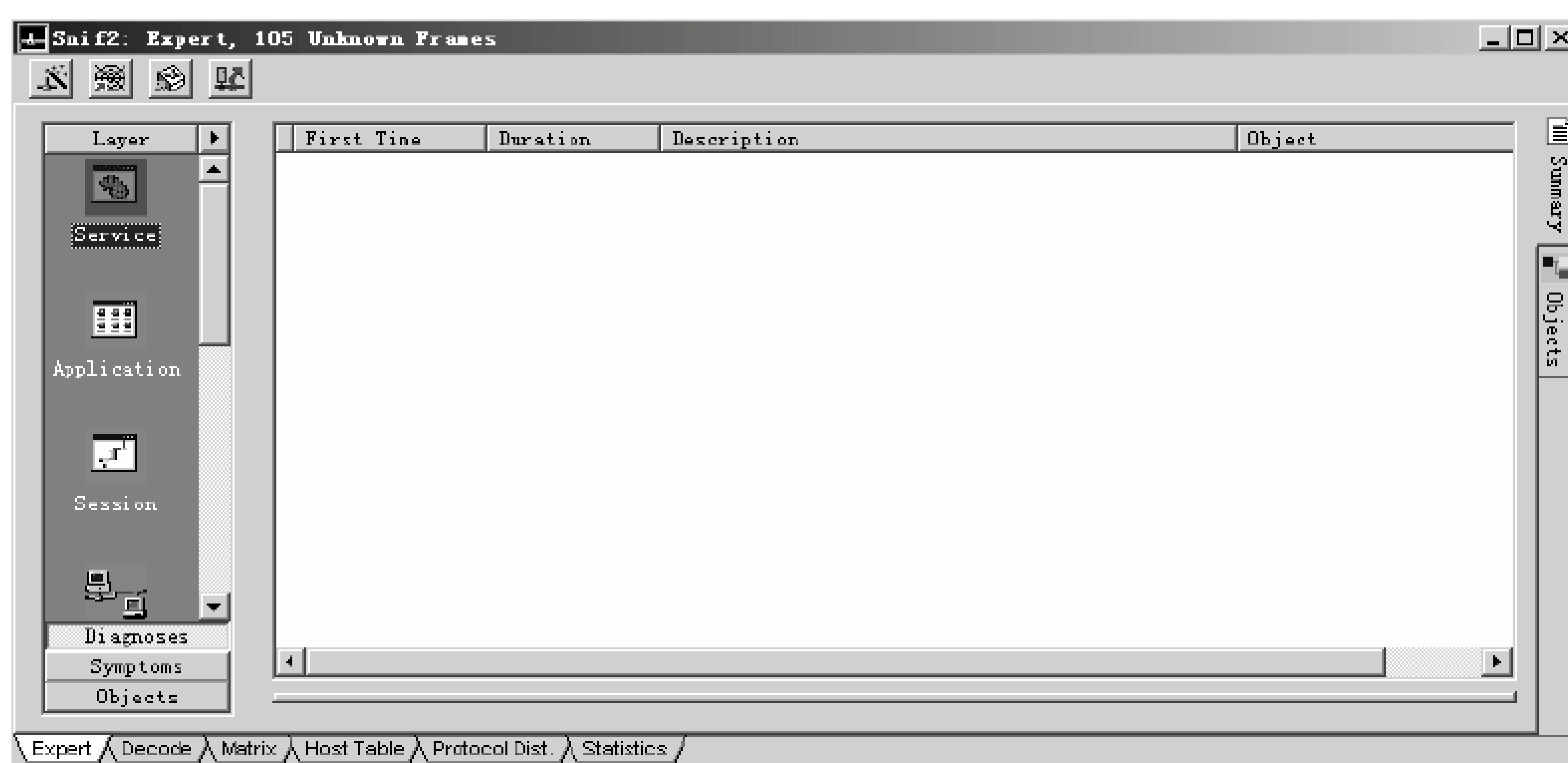


图 18-78 【Snif2：Expert，105 Unknown Frames】窗口

03 单击图 18-80 所示窗口下面的 Decode 标签，进入 Sniffer 的专家解码系统，在其中可以查看相关的数据信息，如图 18-79 所示。

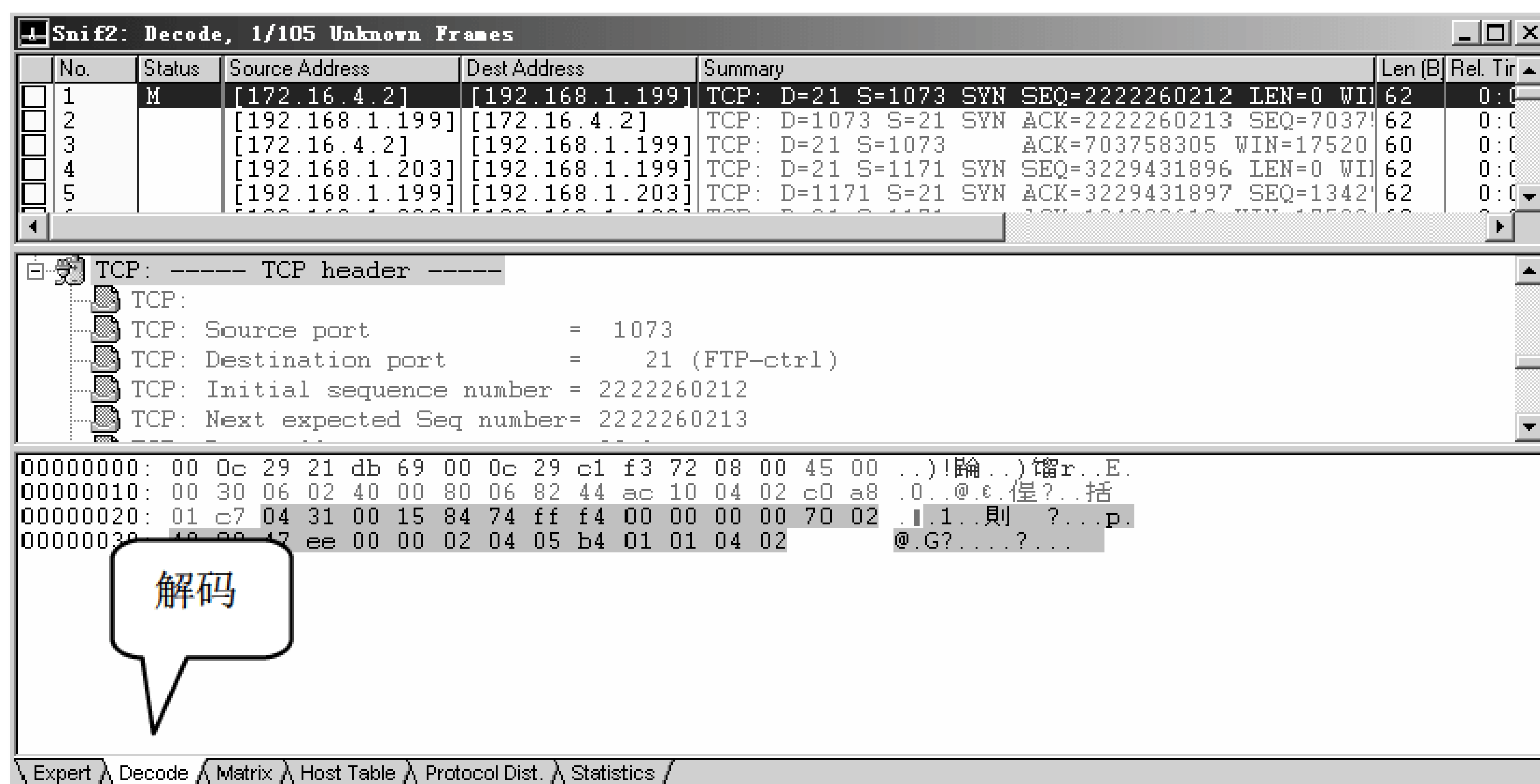


图 18-79 Sniffer 专家解码系统

5. 分析捕捉到的数据包

在 Sniffer Pro 的专家解码界面中，主要分为三部分，从上往下分别是捕捉到的数据包、详细资料、包的十六进制数据信息。

分析捕获到的数据包的具体操作步骤如下。

01 在捕获的数据信息中选择需要分析的数据包信息，如图 18-80 所示为 FTP 数据包。

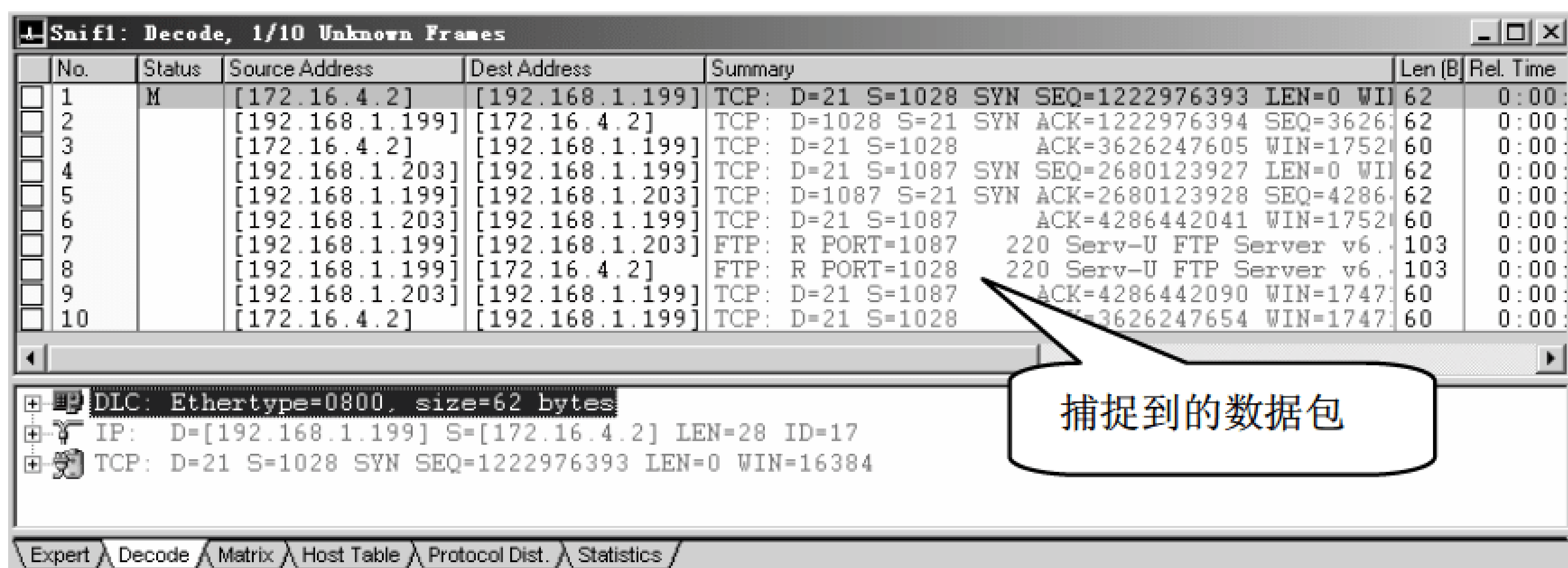


图 18-80 捕获到的 FTP 数据包

图 18-80 所示窗口中的相关参数含义如下：

- No：捕捉到的数据包的序列号。
- Status：捕捉到的数据包的状态。
- Source Address：捕捉到的数据包的源地址。
- Dest Address：捕捉到的数据包的目的地址。
- Summary：捕捉到的数据包的总结信息。

02 单击 DLC（数据链路控制）前面的“+”按钮，展开 DLC 模块，在 DLC 区域中显示了捕捉的帧的数据链路层信息，如图 18-81 所示。

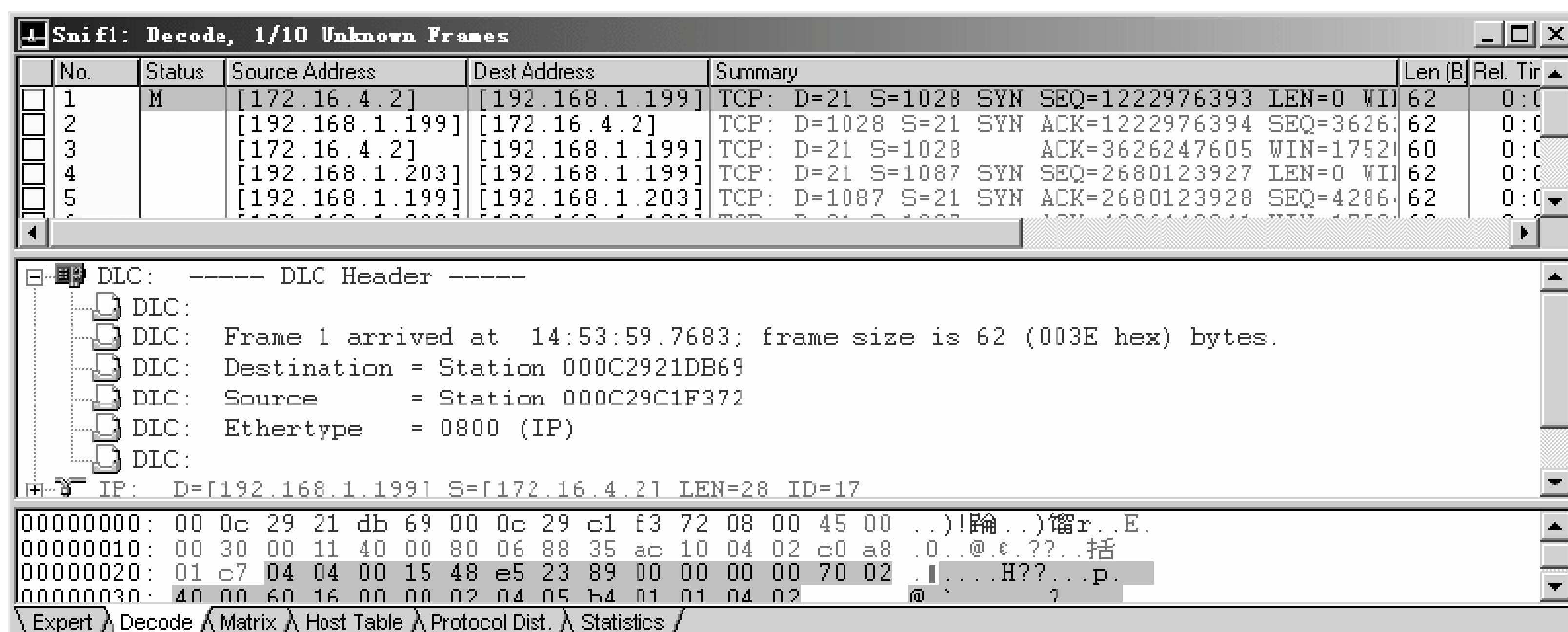


图 18-81 数据包详细信息-DLC 模块

DLC 模块主要包括以下内容。

- Destination：捕捉到的数据的目的物理地址。
- Source：捕捉到的数据包的源物理地址。
- Ethertype：在这里以太类型为 0800，表示是 IPv4。

03 单击 IP 前面的“+”按钮，展开 IP 模块，在 IP 区域中主要显示了捕捉到的数据包的网络层信息，如图 18-82 所示。

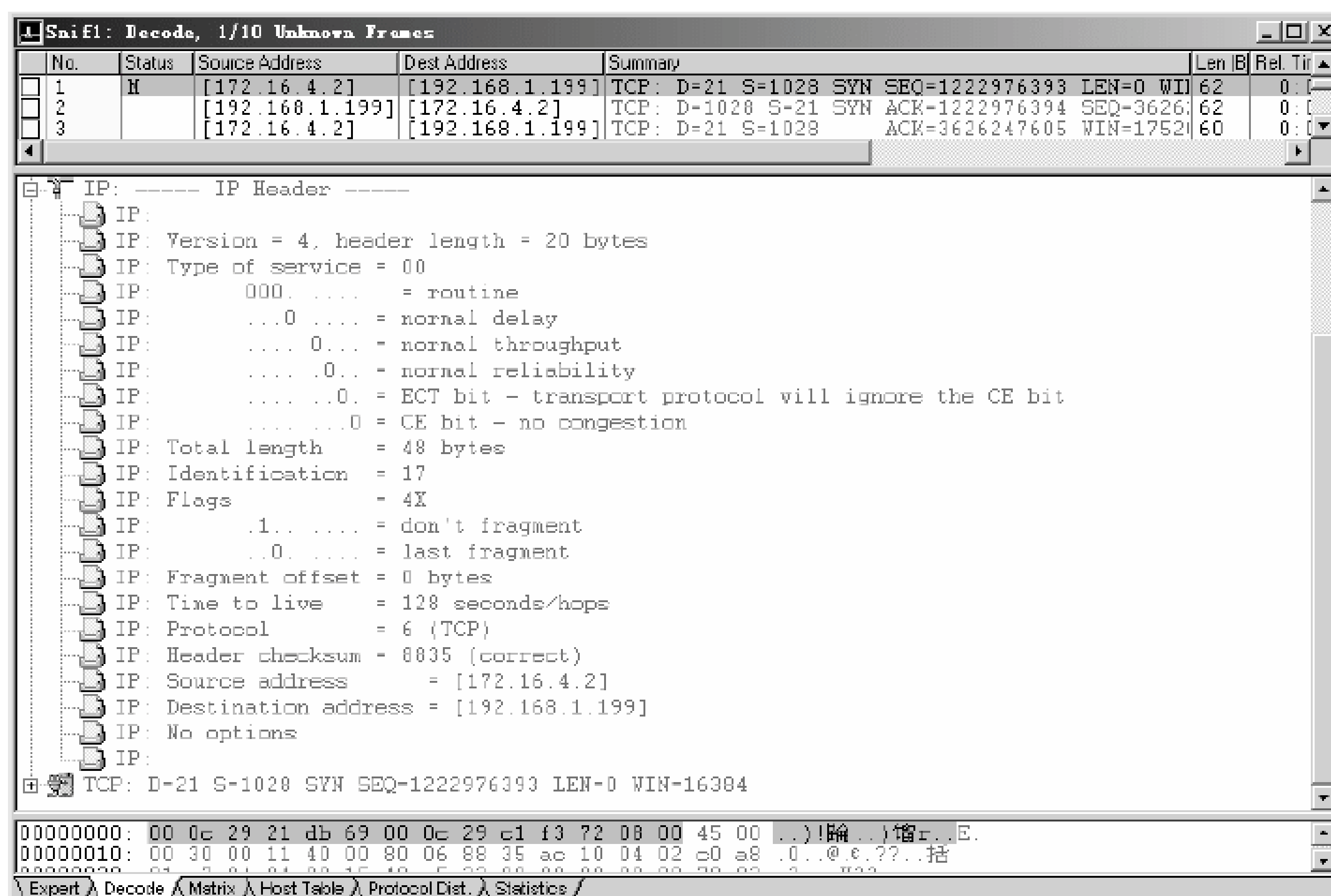


图 18-82 数据包详细信息-IP 模块

IP 模块主要包括以下内容。

- Version：IP 协议的版本，4 表示 IPv4，6 表示 IPv6。
- Total length：IP 数据包的总长度。
- Time to live：表示 TTL 值的大小，说明一个数据包保存时间的长短。
- Protocol：表示这个数据包上一层使用的协议。这里的上一层是传输层，用的是 TCP 协议。
- Source address：数据包的源 IP 地址。
- Destination address：数据包的目标 IP 地址。

04 单击 TCP 前面的“+”按钮，展开 TCP 模块，在 TCP 区域中主要显示了捕捉到的数据包的传输层的相关信息，如图 18-83 所示。

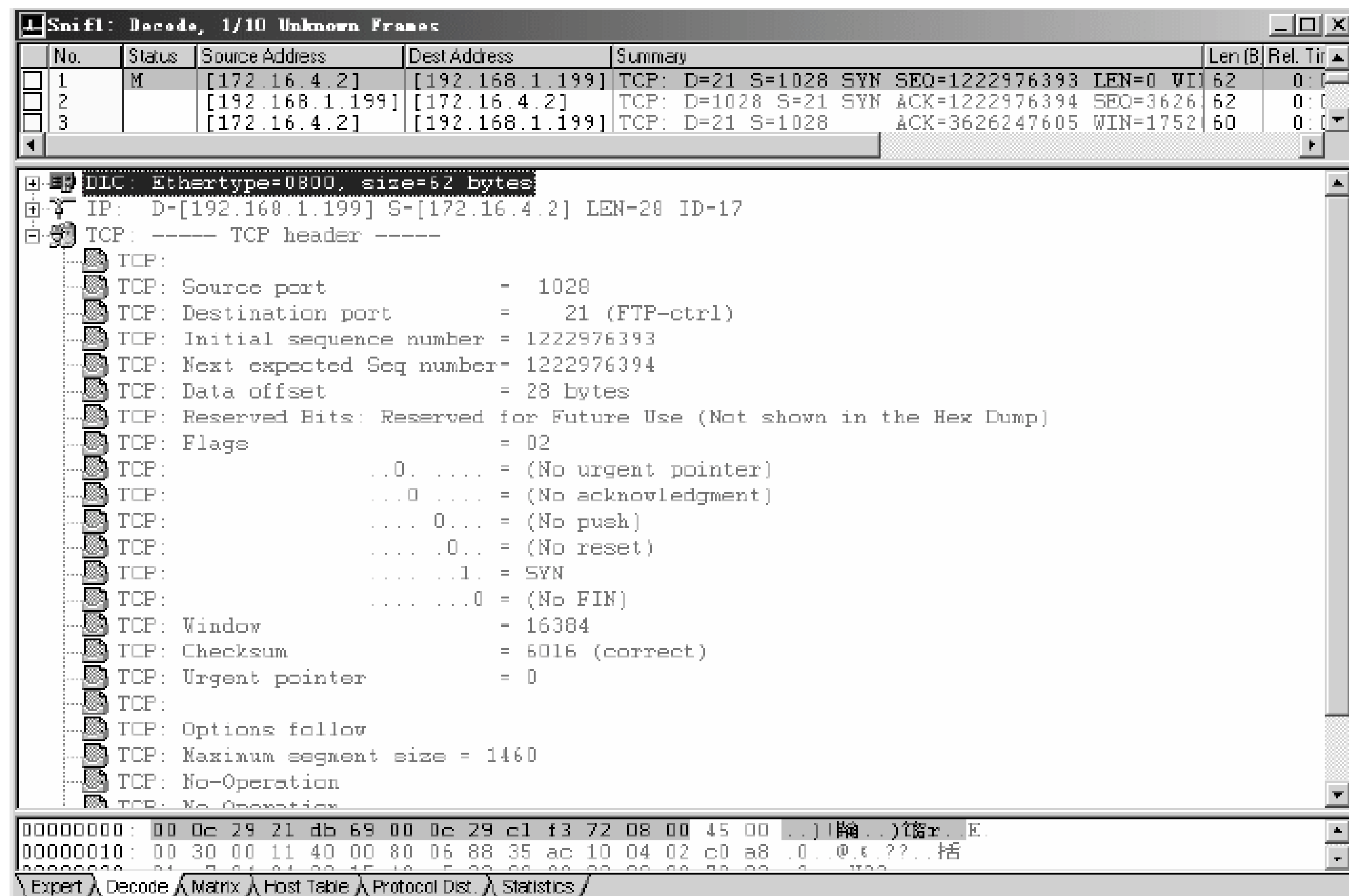


图 18-83 数据包详细信息-TCP 模块

TCP 模块主要包括以下内容。

- Source port：数据包在传输层使用 TCP 源端口号。
- Destination port：数据包在传输层使用的 TCP 目标端口号。
- Checksum：显示了 TCP 协议的校验和。

05 单击图 18-84 所示窗口下方 Matrix 标签，可以直观显示网络中各计算机之间的链接。

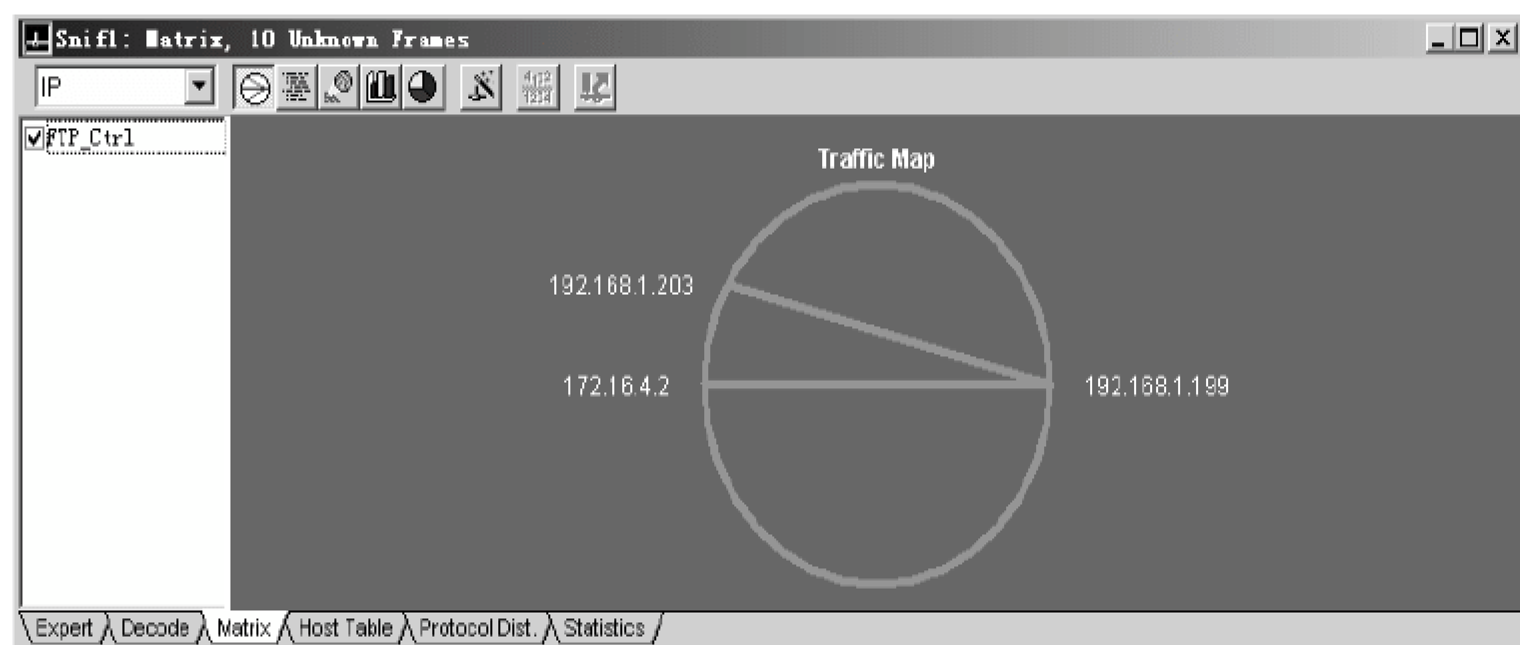


图 18-84　使用矩阵显示计算机连接关系

06 对于捕捉到的数据包，为了便于日后查询或者比较，往往需要保存。当捕捉结束后，在 Sniffer Pro 主操作界面中选择 File ➢ Save 选项，即可将当前已捕捉到的数据包保存在硬盘中。

6. 使用 Sniffer Pro 分析客户端登录 FTP 的过程

网络管理员经常会面临着如何在企业防火墙中设置允许内网主机访问部分外网服务，或者是禁止内网主机访问外网的某个服务的情况，这时就需要详细了解服务的运行信息。Sniffer Pro 可以帮助管理员快速掌握某项服务的数据包的实际流动信息。

下面介绍客户机登录外网 FTP 服务器时的数据包流动情况，具体操作步骤如下。

01 单击 Sniffer Pro 操作界面中工具栏上的 ▶ 按钮，开始捕捉数据包，然后在客户机中的一台计算机上登录 FTP 服务器，如图 18-85 所示。

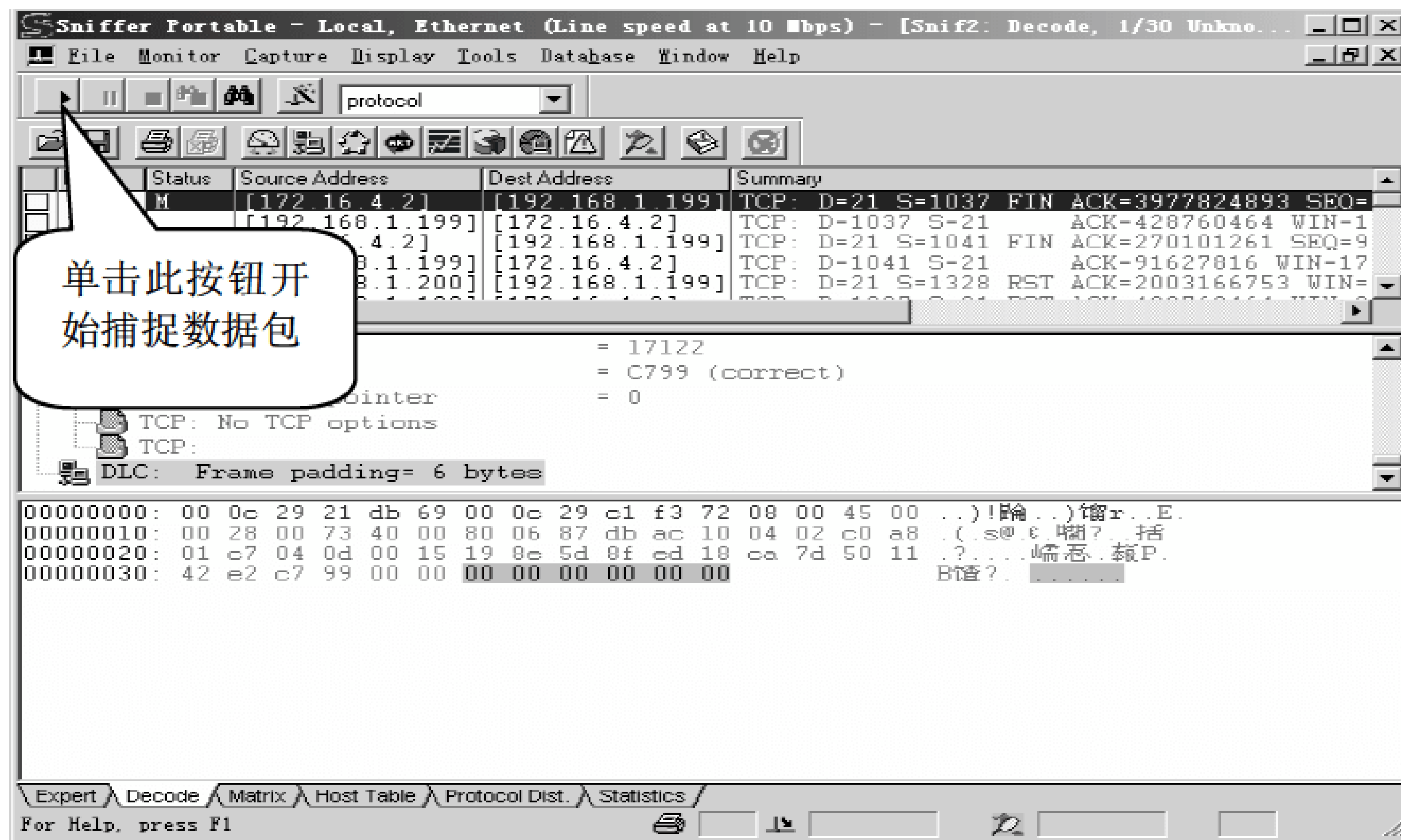


图 18-85　Sniffer Pro 程序主界面

02 当 FTP 登录过程捕捉完成后，单击工具栏上的 按钮，停止捕捉并显示捕捉到的数据包情况，如图 18-86 所示。

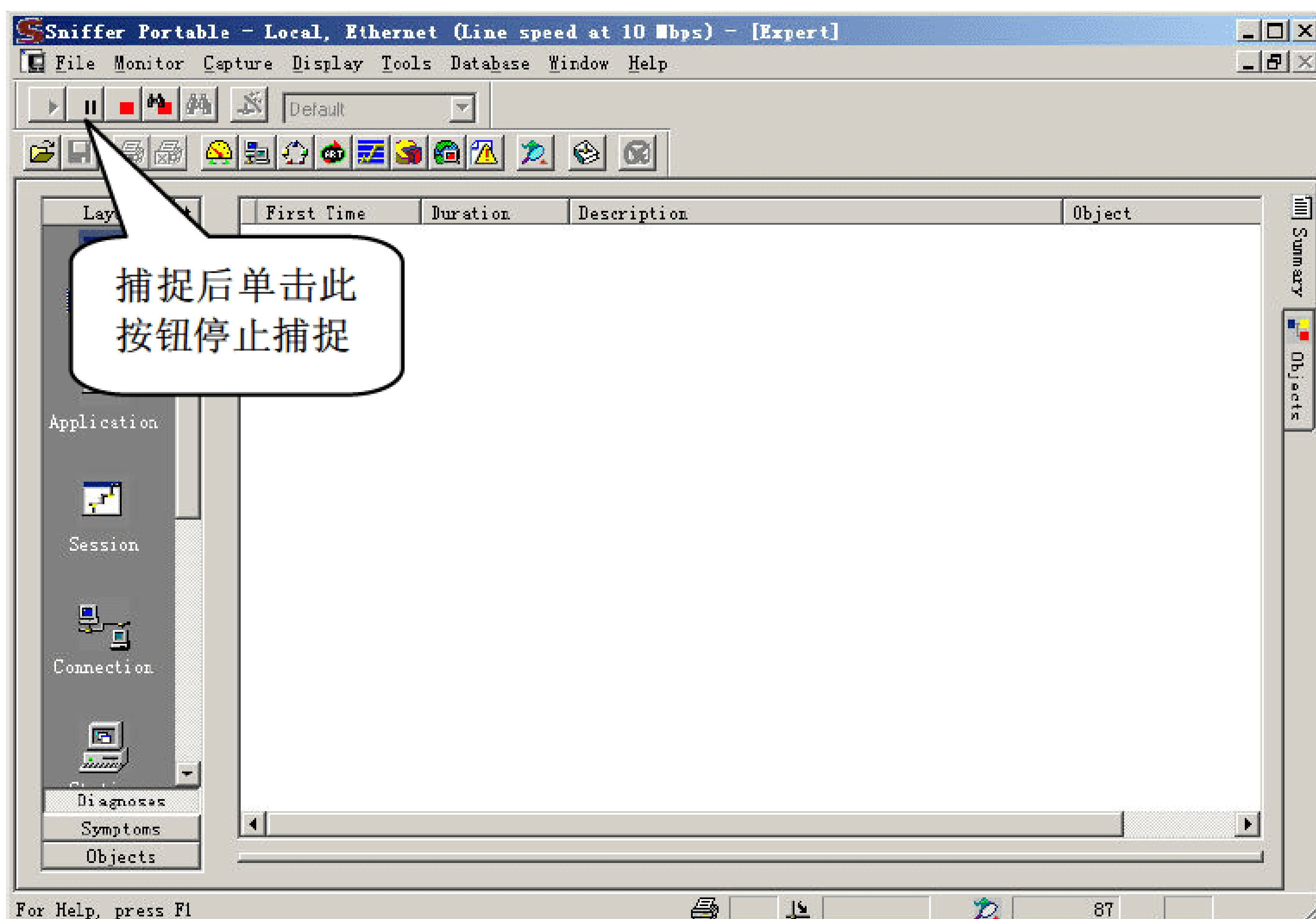


图 18-86　停止捕捉并显示捕捉到的数据包

03 单击选中的 No 为 1 的那个数据包进行分析。可以看到源 IP 为 172.16.4.2 的主机要访问目标 IP 为 192.168.1.199 的 FTP 服务，如图 18-87 所示。

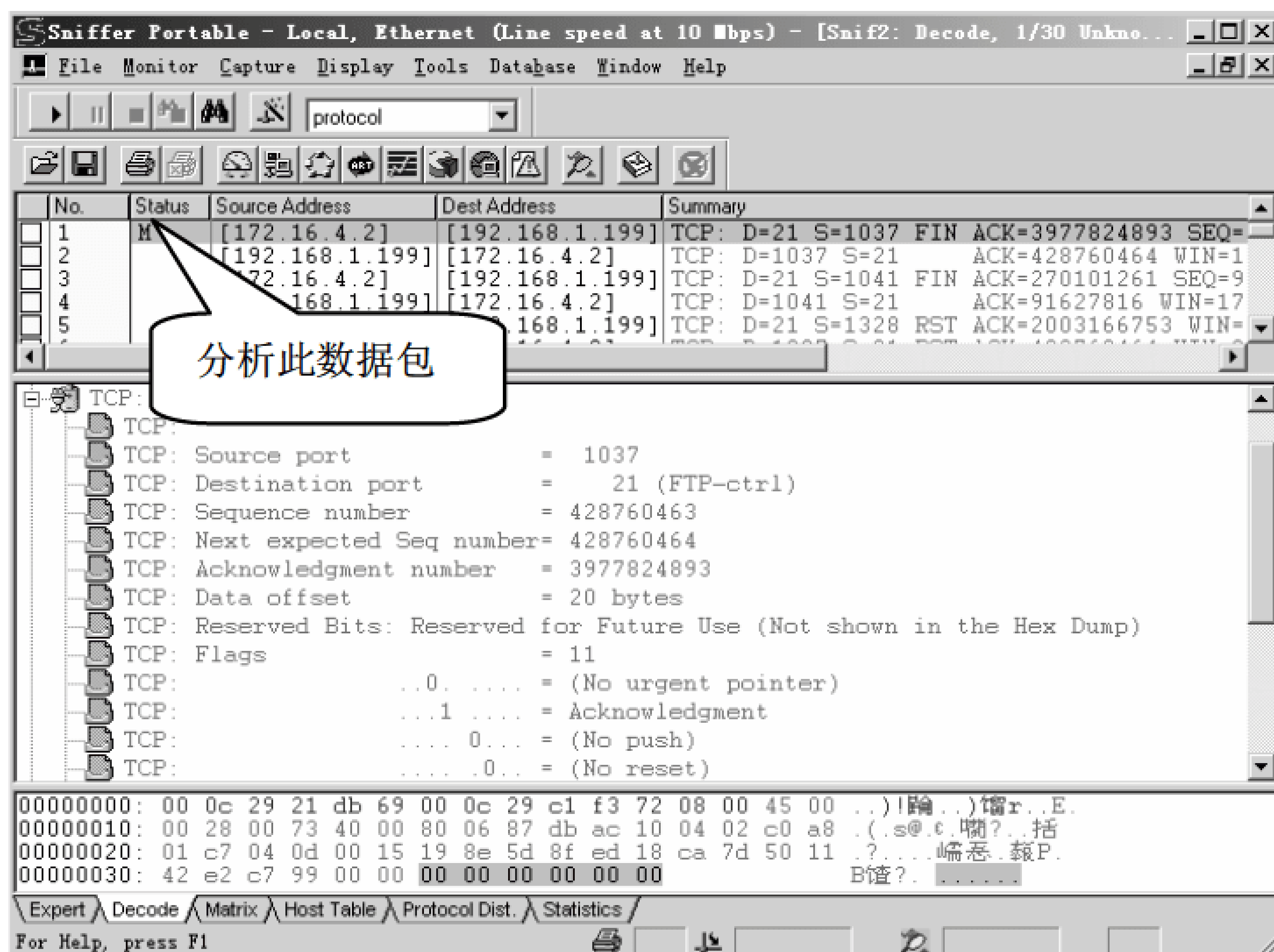


图 18-87　查看捕获的数据包


提　示

通过图 18-89 可以看出该数据包在传输层用的 TCP 协议，其中 Source port（源端口）是 1037，Destination port（目标端口）是 21，因此客户机访问目标主机的 FTP 服务。

04 从捕获到的数据中可以看出 FTP 在传输层使用的是 TCP 协议，在客户机登录 FTP 成功

之前首先需要进行 TCP 协议的三次握手，如图 18-88 所示。

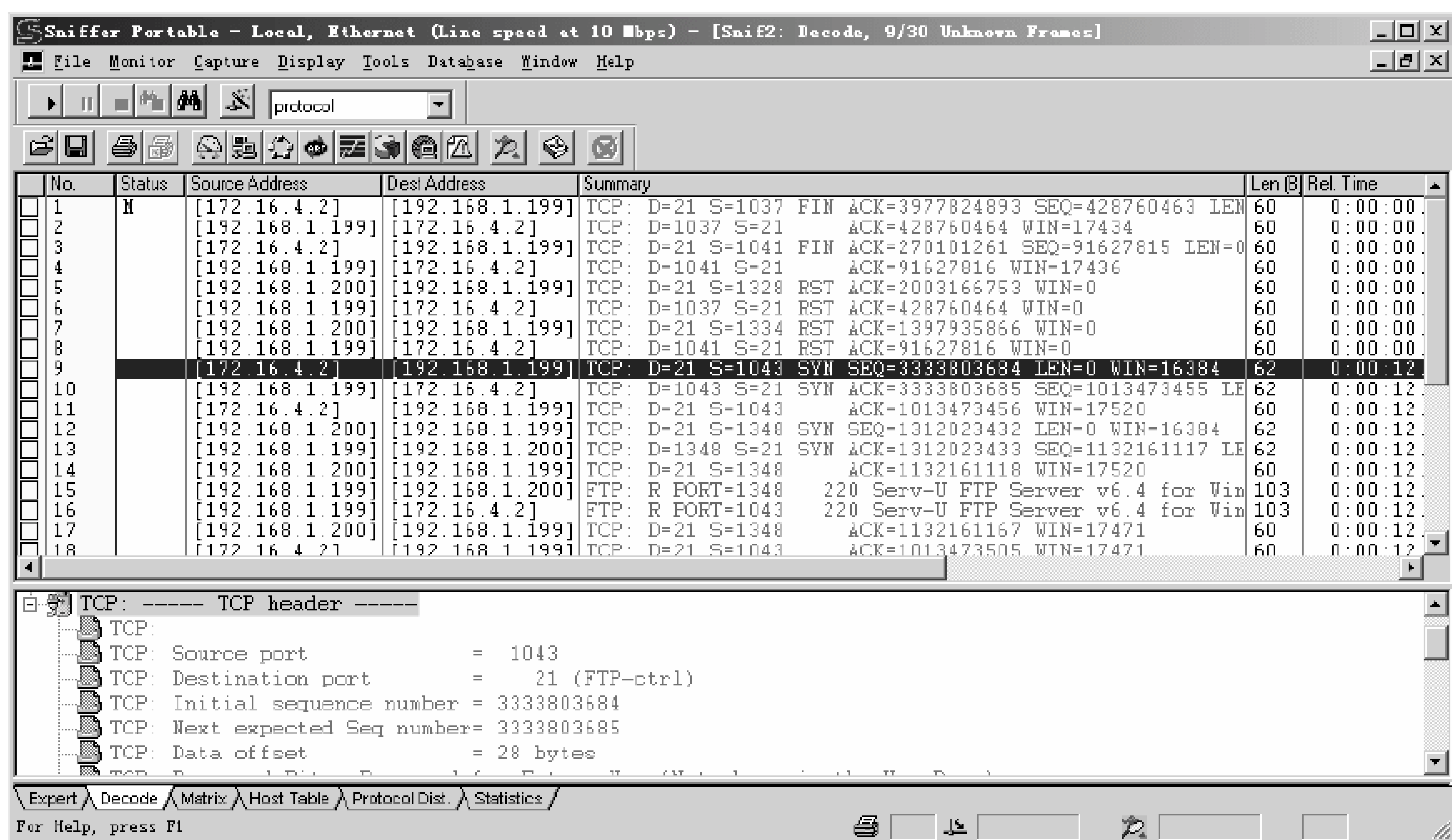


图 18-88　FTP 三次握手流程

结合图 18-88，TCP 三次握手流程分析介绍如下。

- 观察 No 为 9 的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用目标端口 21，源端口 1043 向目标 IP 为 192.168.1.199 的目标主机发送 SYN 同步信息，这是第一次握手。
- 观察 No 为 10 的数据包，可以看出源 IP 为 192.168.1.199 的源主机使用源端口 1043，目标端口 12 向目标 IP 为 172.16.4.2 的目标主机发送 SYN 同步信息和 ACK 确认信息，这是第二次握手。
- 观察 No 为 11 的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用目标端口 1043，源端口 21 向目标 IP 为 192.168.1.199 的目标主机发送 ACK 确认信息，这是第三次握手。

05 从捕获的数据中可以看出登录 FTP 服务器需要对账户和密码进行验证，如图 18-89 所示。

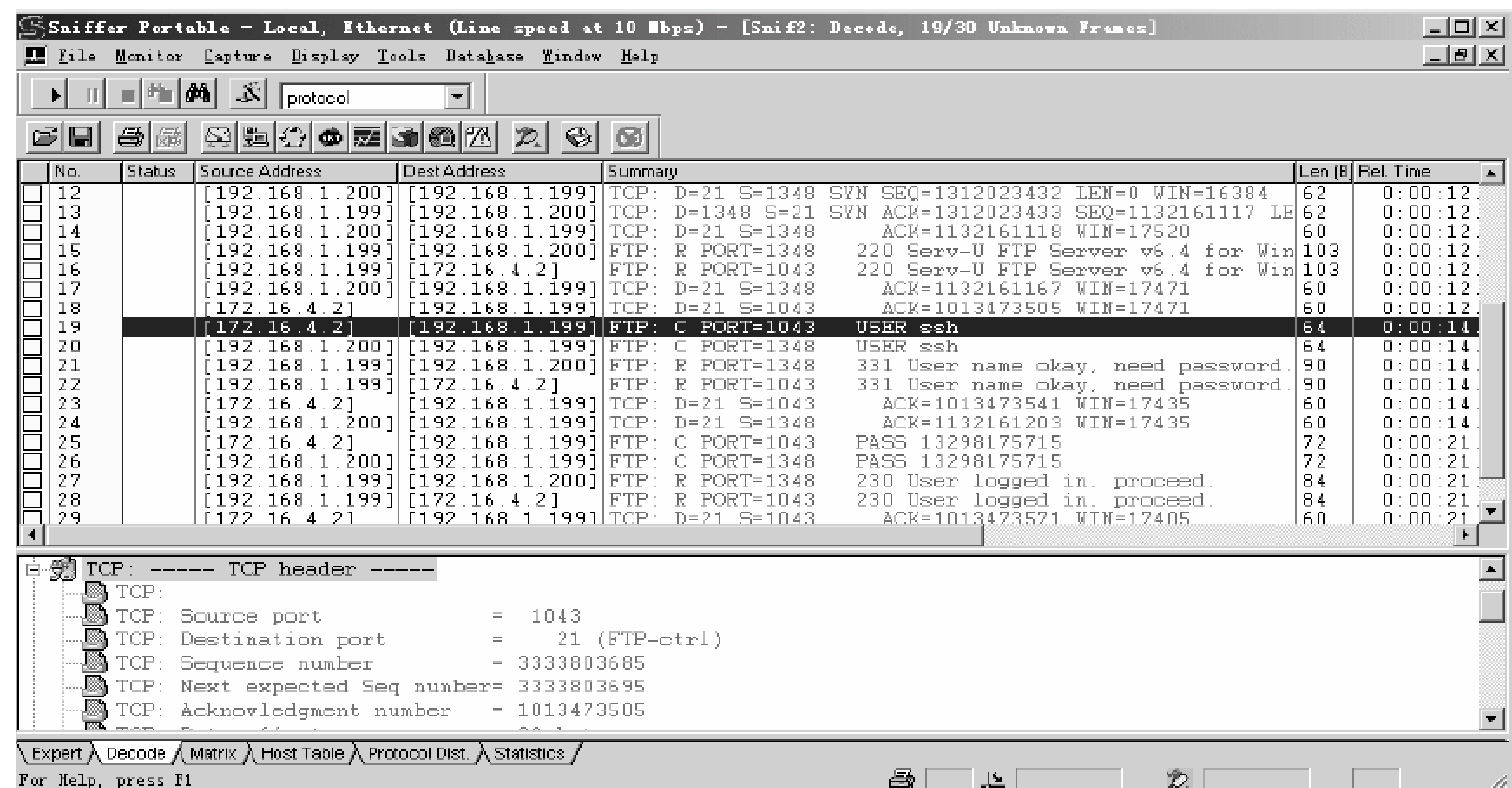


图 18-89　FTP 服务器登录账户验证数据包

结合图 18-89，FTP 身份验证过程分析介绍如下。

- 观察 No 为 19 的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用端口 1043，向目标 IP 为 192.168.1.199 的目标主机发送“USER ssh”意为“用户名为 ssh”的信息。
- 观察 No 为 22 的数据包，可以看出源 IP 为 192.168.1.199 的源主机使用端口 1043，向目标 IP 为 172.16.4.2 的目标主机发送“User name okay，need password”意为“用户名验证通过，需要密码”的信息。
- 观察 No 为 25 的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用端口 1043，目标 IP 为 192.168.1.199 的目标主机发送“PASS 13298175715”意为“密码为 13298175715”的信息。
- 观察 No 为 28 的数据包，可以看出源 IP 为 192.168.1.199 的源主机使用端口 1043，向目标 IP 为 172.16.4.2 的目标主机发送“230 User logged in，proceed”意为“用户登录成功”的信息。

18.4.5　分析造成网络速度慢的原因

在日常的网络管理过程中，经常碰到的问题不是网络不通，而是网络的速度莫名其妙地变得很慢，但是找不到原因。这时可以借助于 Sniffer Pro，通过对 Sniffer 的 HostTable 和 Matrix 进行分析可以清晰找到网络速度慢的原因，具体操作步骤如下。

01 选择 Monitor ➢ HostTable 命令，打开 Sniffer 的主机列表监控功能窗口，可以看到哪些主机在某段时间内传输的数据特别多，如图 18-90 所示。

Sniffer Portable - Local, Ethernet (Line speed at 10 Mbps) - [Host Table: 23 stations]

File Monitor Capture Display Tools Database Window Help

protocol

IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Update Time	Create Time
61.163.78.137	18	17	1,404	1,326	0	0	2011-06-12 17:30:26.229.250	2011-06-12 17:25
192.168.1.166	43	33	3,378	2,787	0	8	2011-06-12 17:30:26.229.250	2011-06-12 17:25
172.16.1.254	512	274	61,860	363,964	0	1	2011-06-12 17:30:24.201.758	2011-06-12 17:25
172.16.4.254	273	512	363,587	61,860	0	0	2011-06-12 17:30:24.201.758	2011-06-12 17:25
60.214.64.135	0	4	0	296	0	0	2011-06-12 17:30:20.589.726	2011-06-12 17:26
183.60.17.90	5	1	320	331	0	0	2011-06-12 17:29:44.998.879	2011-06-12 17:25
234.34.23.234	12	0	792	0	0	0	2011-06-12 17:29:35.617.473	2011-06-12 17:25
239.255.255.250	1	0	377	0	0	0	2011-06-12 17:29:32.941.188	2011-06-12 17:29
192.168.1.86	0	4	0	264	0	4	2011-06-12 17:29:21.788.774	2011-06-12 17:25
224.0.0.22	1	0	64	0	0	0	2011-06-12 17:29:07.650.567	2011-06-12 17:29
192.168.1.243	0	1	0	64	0	1	2011-06-12 17:29:07.650.567	2011-06-12 17:29
BROADCAST	5	0	408	0	0	0	2011-06-12 17:29:05.787.827	2011-06-12 17:25
192.168.1.203	14	3	21,252	274	3	0	2011-06-12 17:29:05.787.827	2011-06-12 17:25
192.168.1.199	9	0	582	0	0	0	2011-06-12 17:28:49.701.63	2011-06-12 17:27
192.168.1.200	0	5	0	320	0	0	2011-06-12 17:28:49.701.63	2011-06-12 17:28
61.54.220.74	0	14	0	21,252	0	0	2011-06-12 17:28:49.396.562	2011-06-12 17:28
125.39.150.21	0	1	0	64	0	0	2011-06-12 17:28:47.112.464	2011-06-12 17:28
125.41.136.92	0	19	0	1,266	0	0	2011-06-12 17:28:33.973.56	2011-06-12 17:27
172.16.4.2	0	3	0	196	0	0	2011-06-12 17:28:27.457.197	2011-06-12 17:27
192.168.1.247	0	2	0	134	2	0	2011-06-12 17:28:26.785.628	2011-06-12 17:28
192.168.1.75	1	0	442	0	0	0	2011-06-12 17:27:59.436.921	2011-06-12 17:27
172.16.4.1	0	1	0	66	0	0	2011-06-12 17:27:27.81.553	2011-06-12 17:27
60.216.233.171	1	1	93	95	0	0	2011-06-12 17:27:06.77.180	2011-06-12 17:27

MAC IP IPX

For Help, press F1　　12

图 18-90　Sniffer 的主机列表监控功能窗口

02 选择 Monitor ➢ Matrix 菜单命令，打开 Sniffer 的矩阵监控功能。通过 Matrix 矩阵监控功能查看数据传输特别多的那些主机都在和什么主机通信，如果发现这些主机在某些特定的时段传输数据量特别大并且是和大量的不同主机进行并发连接，这时候怀疑是这些主机在进行 P2P、BT 下载或者是中了蠕虫病毒，导致大量并发通信，使网络效率降低，影响网速，如图 18-91 所示。

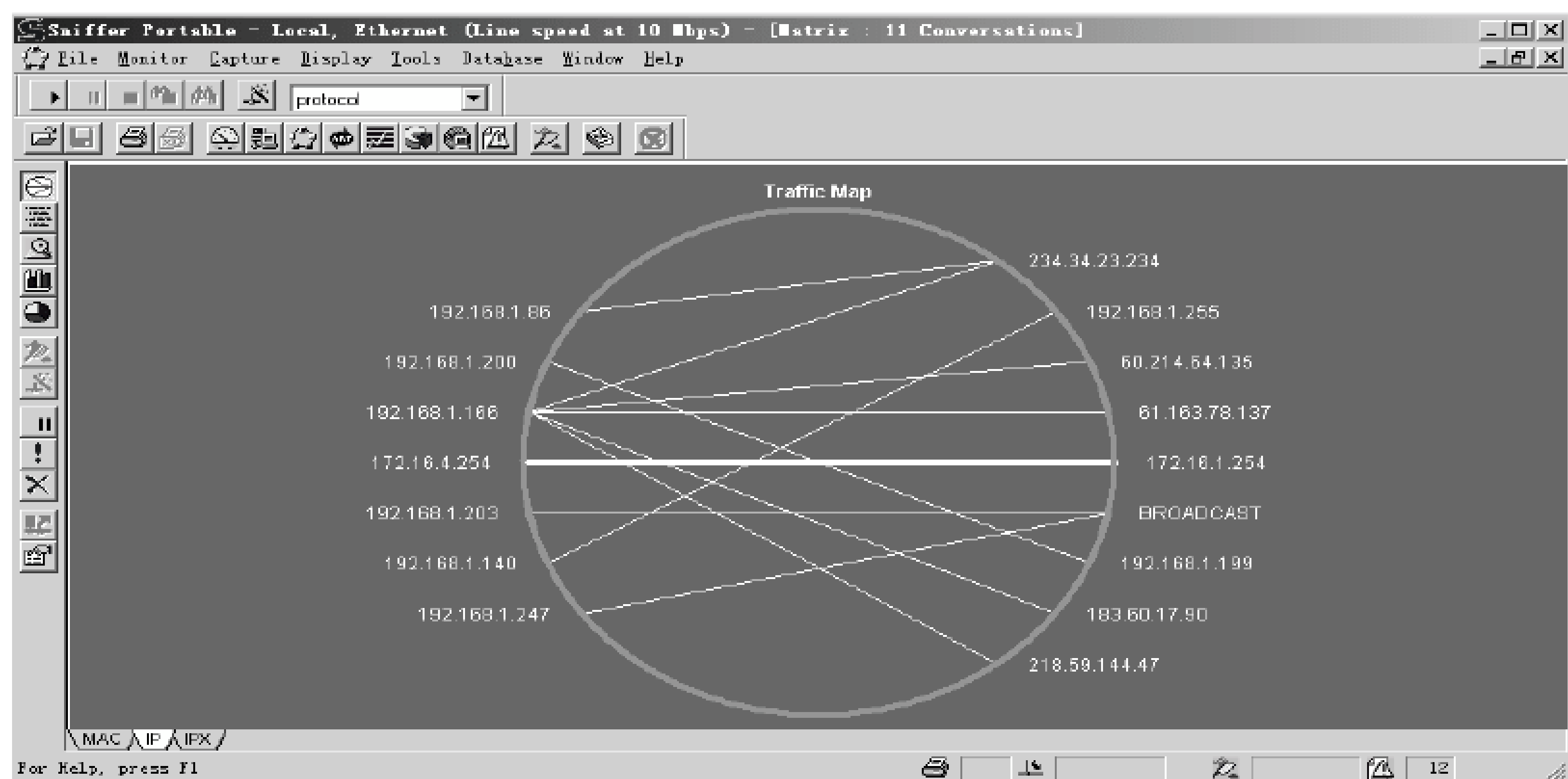


图 18-91　Sniffer 的矩阵监控功能

18.4.6　查找网络 ARP 攻击源

在局域网通信的过程中，当源主机在请求 ARP 解析的时候，ARP 攻击者伪装目的主机的 MAC 地址返回给源主机，这时候源主机就会对接收到的错误目标 MAC 地址进行访问，使得网络内部出现大量的无用广播流量影响网络效率，这就是 ARP 攻击或者 ARP 欺骗。

通过 Sniffer Pro 查找网络 ARP 攻击源的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面选择 Capture ➢ Define Filter 命令，弹出 Define Filter – Capture 对话框，单击 Profiles 按钮，如图 18-92 所示。

02 弹出 Capture Profiles 对话框，单击 New 按钮，如图 18-93 所示。

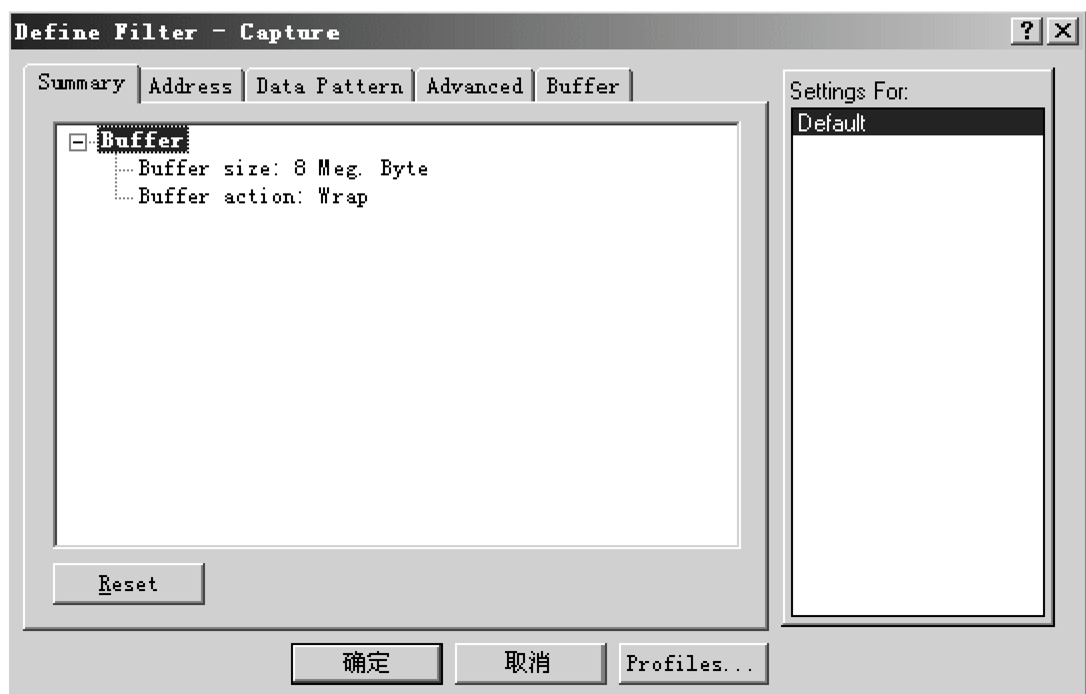


图 18-92　Define Filter – Capture 对话框

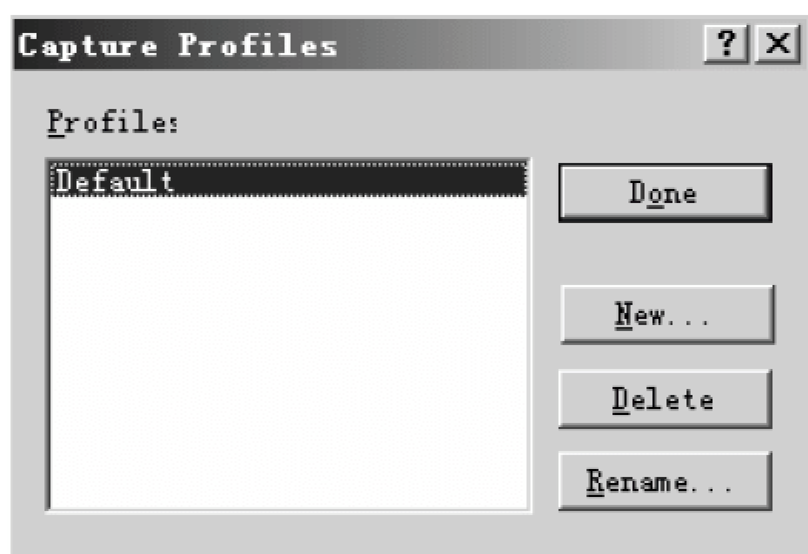


图 18-93　Capture Profiles 对话框

03 弹出 New Capture Profile 对话框，在 New Profile Name 文本框中输入过滤器的名称 ARP，单击 OK 按钮，一个新的过滤器创建完成，如图 18-94 所示。

04 返回 Capture Profiles 对话框，单击 Done 按钮，如图 18-95 所示。

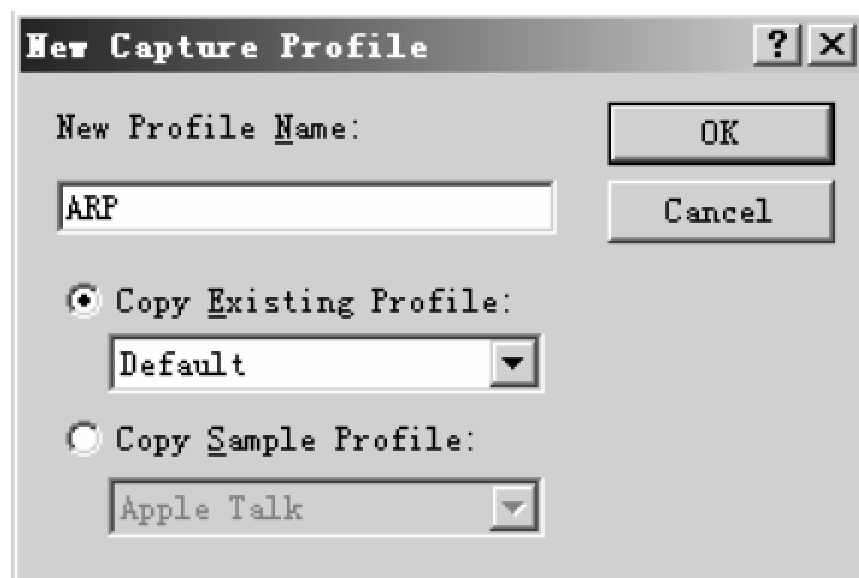


图 18-94　New Capture Profile 对话框

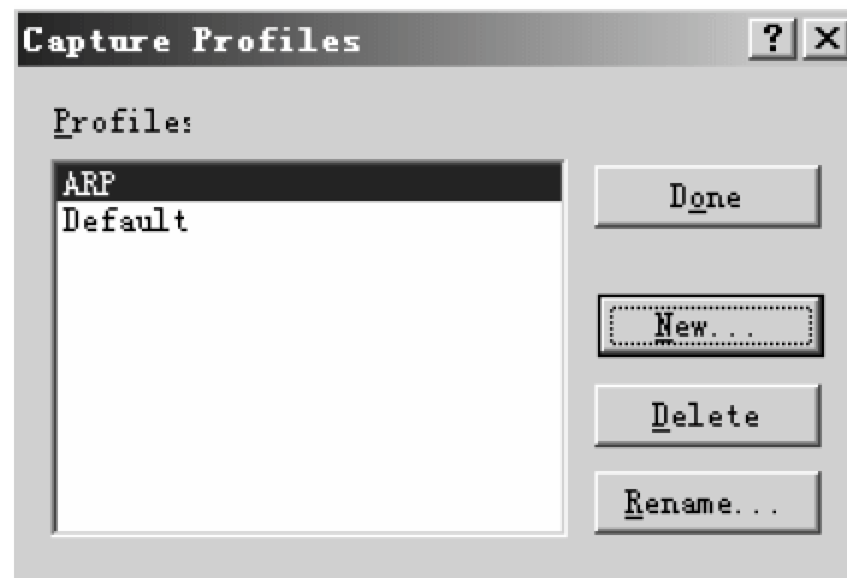


图 18-95　Capture Profiles 对话框

05 返回 Define Filter – Capture 对话框，选择 Advanced 选项卡，选中 IP ARP 协议，一个新的 ARP 协议过滤器创建完成，如图 18-96 所示。



图 18-96　选择 IP ARP 协议

06 单击工具栏上的▶按钮，开始捕捉数据包，如图 18-97 所示。

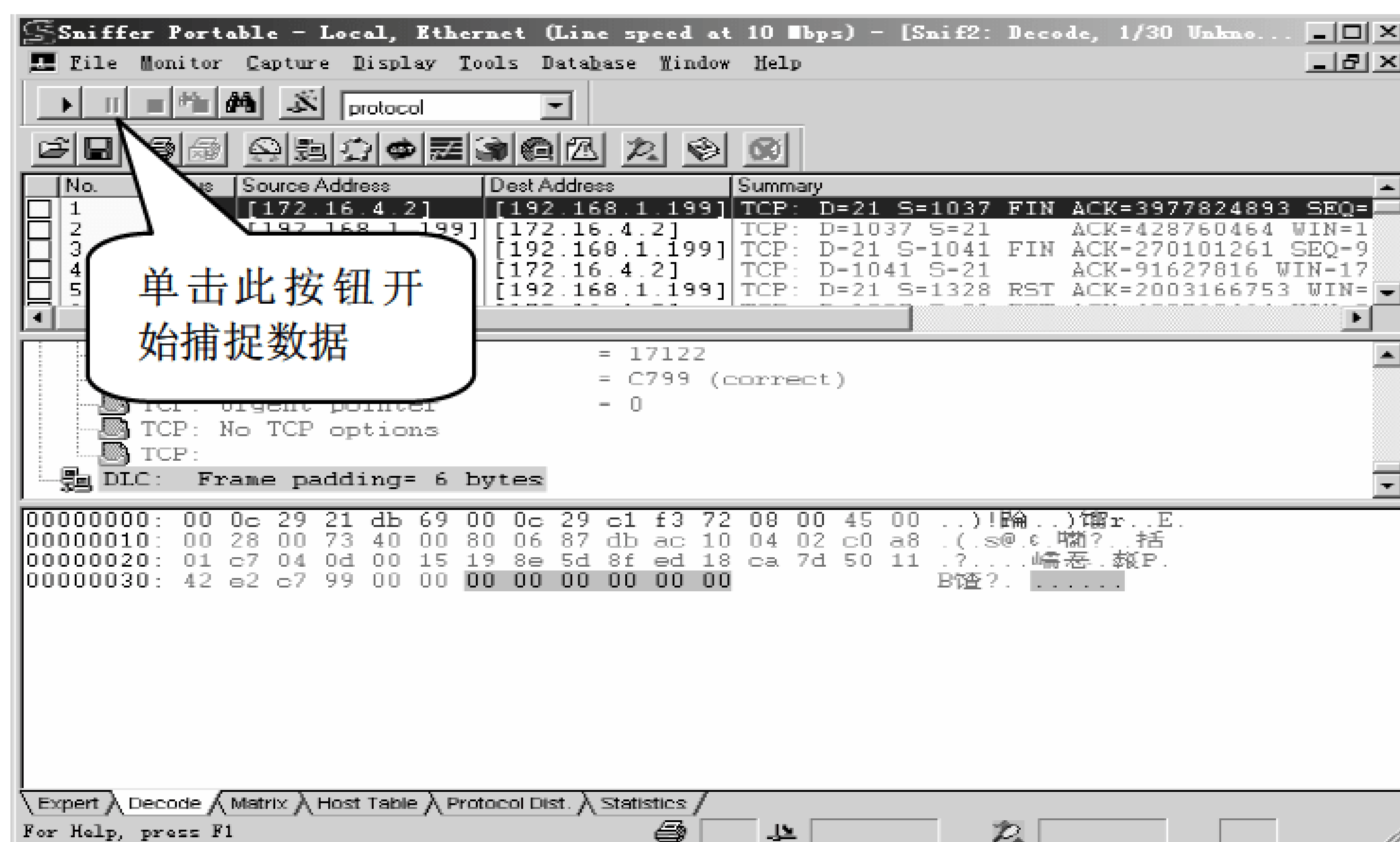


图 18-97　捕捉数据包

07 过一段时间后单击工具栏上的按钮，停止捕捉并显示捕捉到的数据包情况，如图 18-98 所示。

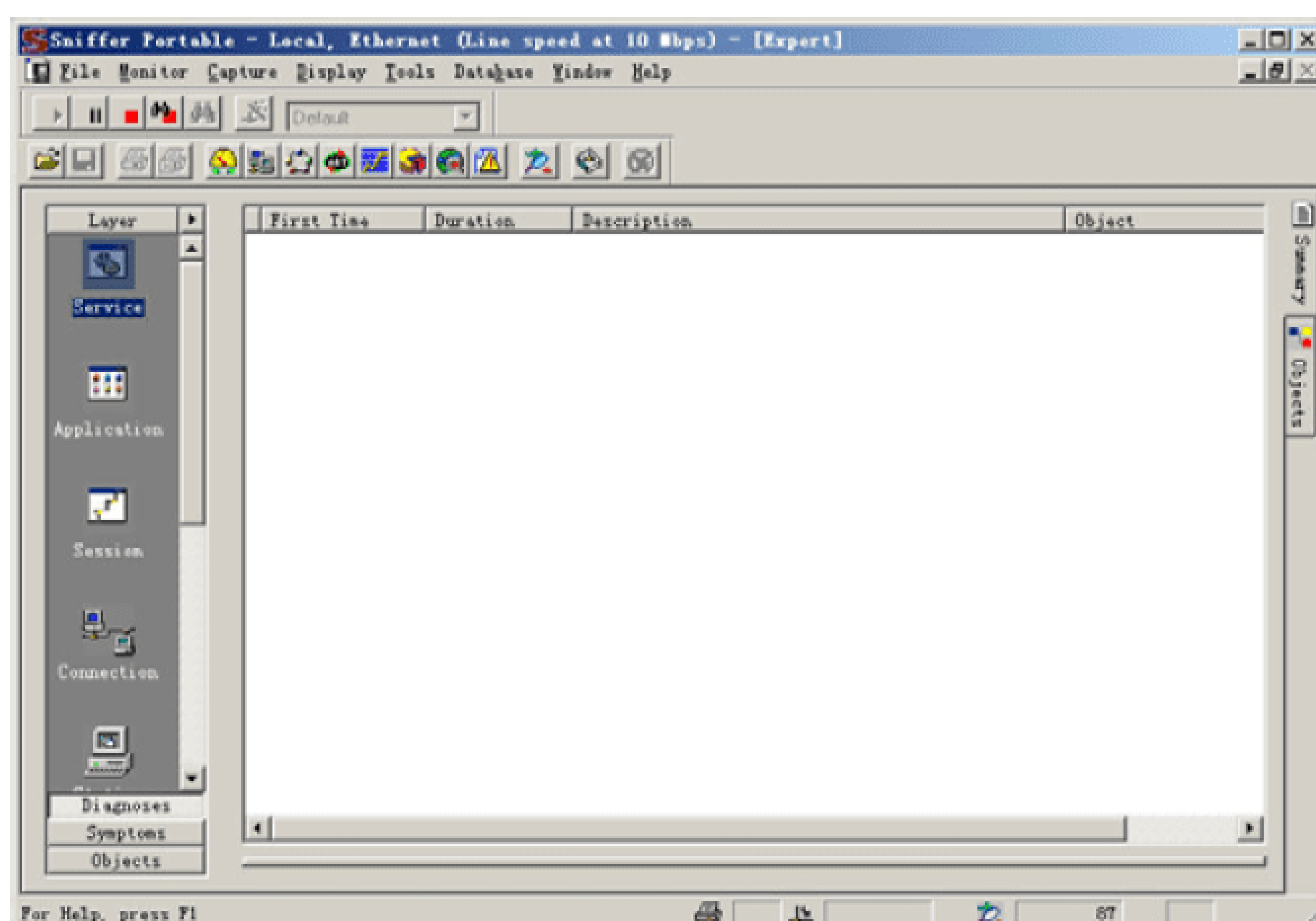


图 18-98　停止捕捉并显示捕捉到的数据包

08 选择 Monitor ➢ Matrix 命令，打开 Sniffer 的矩阵监控功能，如图 18-99 所示。

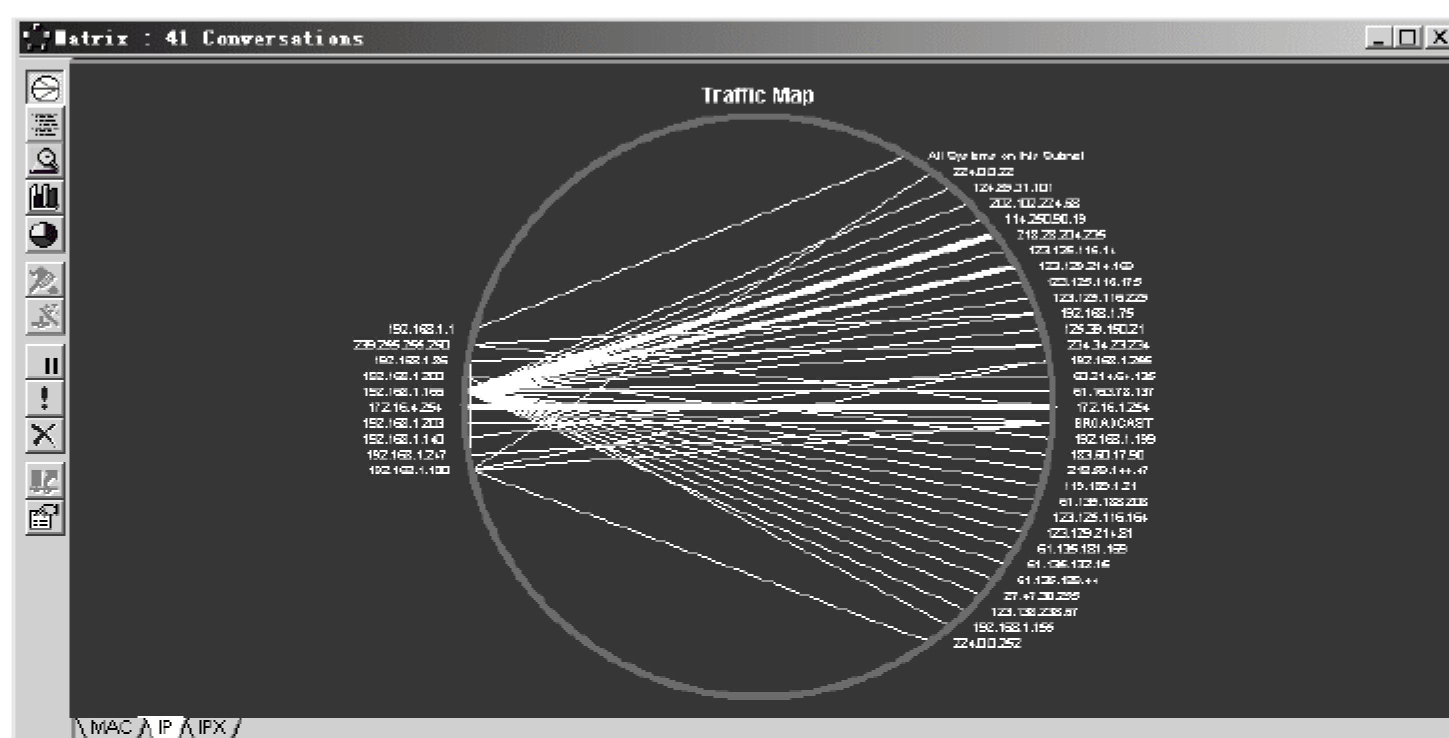


图 18-99　Sniffer 的矩阵监控功能



观察图 18-101 中的数据通信，如果发现有某一个主机正在和局域网内大量的主机进行并发连接，那么怀疑该主机中了 ARP 病毒或者受到人为的 ARP 攻击，网络管理员应该及时找到该主机采取相应措施。

09 在复杂的网络环境中，如果要查看某个单独的主机通信情况，如查看 IP 为 192.168.1.199 的主机通信情况，右击“192.168.1.199”，在弹出的快捷菜单中选择 Show Select Node（显示选择的节点）命令，如图 18-100 所示。

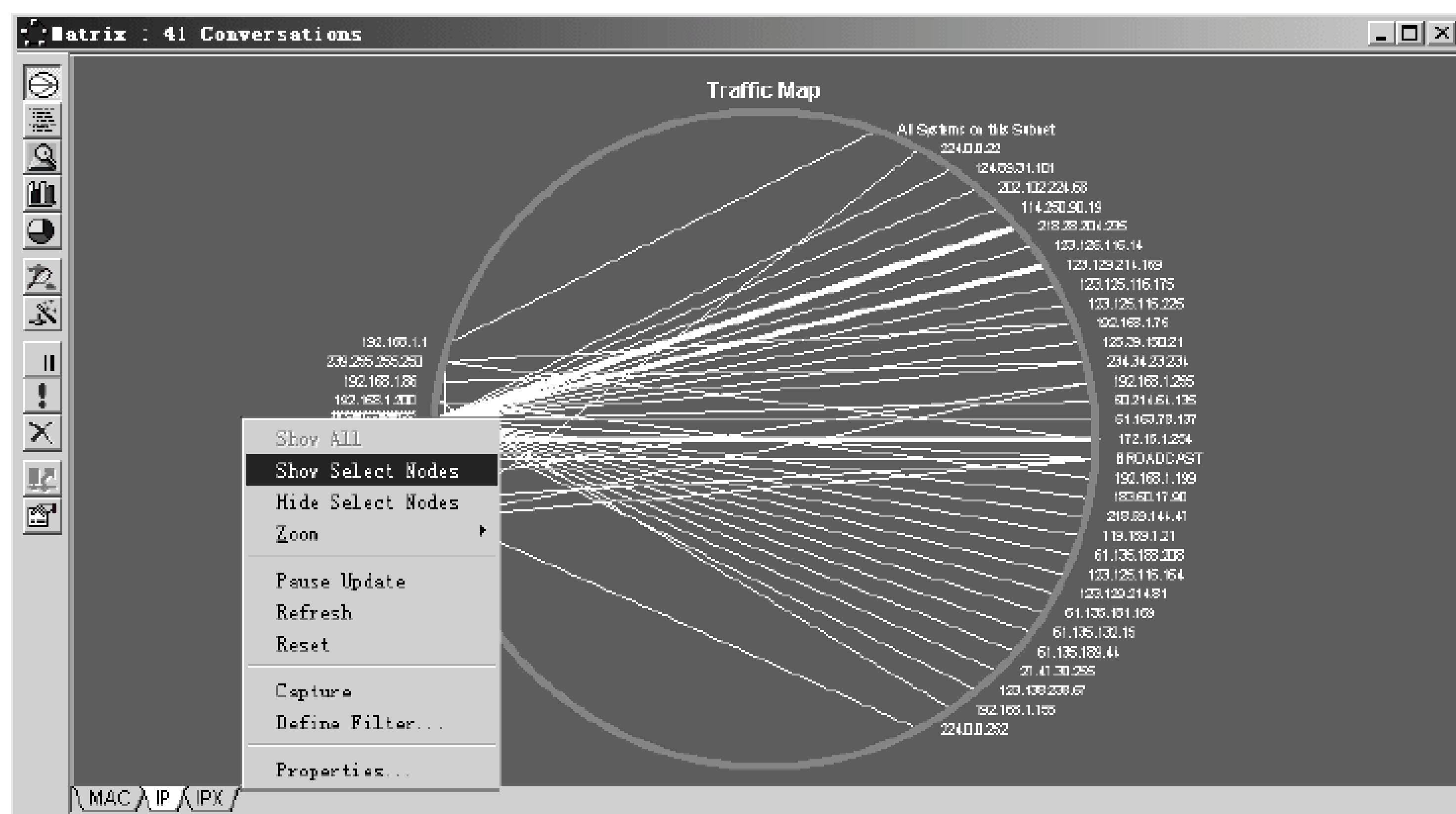


图 18-100　显示选择的节点

10 弹出 IP 为“192.168.1.199”的主机的通信情况的矩阵信息，如图 18-101 所示。

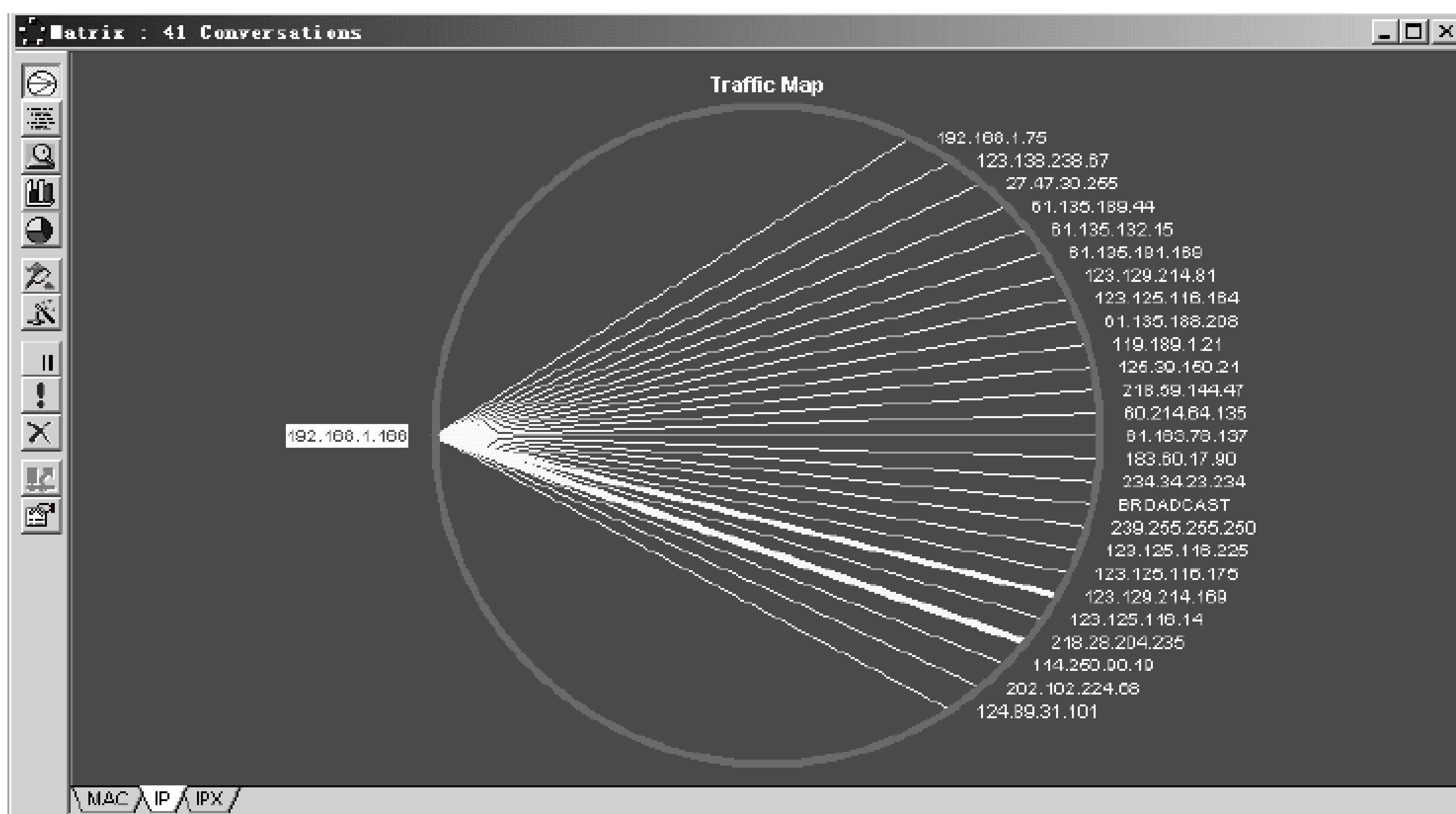


图 18-101　只显示一个主机的通信矩阵信息


提　示

如果该主机正在和大量的外网主机并发通信并有大量的数据包传输出现，就有可能是该主机正在进行 P2P、BT 等下载，如果该主机正在和大量内网主机并发通信，则有可能中了 ARP 病毒、蠕虫，或者是人为安装了 P2P 攻击软件，并且正在进行 ARP 攻击，这时网络管理员就可以根据 IP 或者 MAC 地址找到该主机，然后采取相应措施。

18.5　专家答疑

（1）安装 Sniffer Pro 软件后，打开软件包时软件的界面显示不完整，或者有时候网页会显示不完整，怎样解决？

答：Sniffer Pro 的界面显示需要 Java 的 JDK 支持，安装 JDK 即可，有的时候安装 JDK 后再打开 Sniffe Pro 会出现网页错误的提示，这是因为计算机的 IE 版本过低，升级 IE 版本即可。

（2）安装 Sniffer Pro 后进行数据包的捕捉，可是 Capture 菜单中的 Stop and Display 选项是灰色的，使得无法停止数据包的捕捉，怎么办？

答：关于捕捉数据包后无法停止数据包的捕捉的问题，一般是因为 Sniffer Pro 没有正常捕捉到数据包，这时候就需要考虑 Sniffer Pro 的安装位置是否合适，或者是 Sniffer Pro 监听网卡没有监听到数据包。

第 19 章　企业网络病毒防护系统架设与使用

随着互联网的不断发展，病毒也不断演变，新型病毒层出不穷，在网络传播能力和破坏力方面表现得也越来越强劲。因此，反病毒已经成为企业信息安全非常重要的一环。特别是在企业网络里，用户群比较多，安全需求也高，一旦有病毒传播只靠单一主机自主查杀是没有意义的。面对企业网络的病毒威胁，网络管理员必须做更多的考虑，选择更智能、更全面、更系统的企业反病毒系统。

19.1　反病毒系统概述

在搭建企业反病毒系统之前，先来了解一下什么是企业反病毒及其分类、设计原则等信息。

19.1.1　企业反病毒的定义

企业反病毒是针对企业网络反病毒需要而提出的一套可以实时监控网络安全状态并能实现全网病毒查杀的反病毒系统。

要想深刻地了解什么是企业反病毒，首先要把企业反病毒和通常个人家庭使用的杀毒软件区分开。例如，常见的家庭个人使用的瑞星、360、卡巴斯基、金山等杀毒软件都是针对单个主机查杀病毒的，这就不是企业反病毒。常见的企业反病毒有诺顿企业版、ESET NOD32 企业版、卡巴斯基企业版、360 杀毒企业版、趋势科技等。

19.1.2　企业反病毒系统的设计原则

面对如此严峻的网络安全形势，各大企业对网络信息安全防护也越来越重视，并纷纷投入大笔资金进行网络安全产品的采购和部署。但是设备只是信息安全防护的骨架，应该有合理的、统一的防范策略作保障。所以在架设反病毒系统时需要进行严格的、深入的分析和设计。

下面详细介绍企业防病毒系统的设计原则。

1. 满足查杀中国式病毒要求

文化有国界特色，病毒也不例外，中国式病毒在网络安全部署过程中是不容忽视的。所以在进行反病毒系统设计时也需要考虑中国特色。

国际上知名的老牌杀毒软件，拥有强大的软硬件技术，但是面对中国式病毒它也无能为力。

2006—2007 年比较流行的熊猫烧香病毒，大都是依靠 360 等多款国内杀毒软件推出的专杀程序解决的。不是说国外杀毒软件不好，只是在针对中国特色的病毒上，它们没有突出的优势。

所以在国内网络中可以使用国内知名的老牌杀毒软件，但是也要在此基础上做好中国式病毒查杀的补充。

2. 保证对新病毒的查杀能力

杀毒软件并不是安装之后就不用管了，随着新病毒、木马的不断出现，杀毒软件也必须及时更新程序和病毒库。如果不能实现快速的升级和病毒库更新，新病毒就会以其惊人的传播速度和破坏力毁灭整个网络的计算机，给企业带来巨大的损失。所以保证杀毒软件快速的升级和响应是体现其病毒查杀能力的决定性因素之一。

杀毒软件的升级和病毒库更新由三方面因素决定，分别为软件因素、管理因素和网络因素。

（1）软件因素：不同的软件应对新病毒的更新速度不相同，选择一款更新及时的杀毒软件很重要，很多软件可以做到一天几次的更新频率。

（2）管理因素：很多杀毒软件被设置更新需要管理员手动操作，如需要管理员确认更新提示等，这样会影响更新速度，一般建议设定自动更新，且每天做一次手动更新。

（3）网络因素：网络环境通畅与否也直接影响更新效率，如网络经常处于拥塞、速率低等状态。

19.2 项目实战 1：ESET NOD32 企业反病毒系统实战案例

ESET NOD32 作为知名的企业反病毒系统，具有较高的市场占有率。下面介绍 ESET NOD32 企业反病毒系统的架设及应用。

19.2.1 安装 ESET NOD32 企业反病毒系统

ESET NOD32 企业反病毒系统主要由三部分程序组成：ESET NOD32 防病毒软件、ESET 远程管理服务器、ESET 远程管理控制台，三个软件可以通过官方网站下载获得。

企业内所有客户机都需要安装 ESET NOD32 防病毒软件，同时需要指定一台主机安装 ESET 远程管理服务器和 ESET 远程管理控制台程序作为企业反病毒系统的管理服务器。

下面分别介绍三种程序的安装过程。

1. 安装 ESET NOD32 企业版防病毒软件

安装 ESET NOD32 防病毒软件之前，一定要确保本机没有其他安全防护程序，如病毒防护和间谍软件防护程序。

安装 ESET NOD32 防病毒软件的具体操作如下。

01 运行 ESET NOD32 防病毒软件安装程序，弹出安装向导对话框，单击【下一步】按钮，如图 19-1 所示。

02 弹出【最终用户许可协议】对话框，选中【我接受许可协议中的条款】单选按钮，单击

【下一步】按钮，如图 19-2 所示。

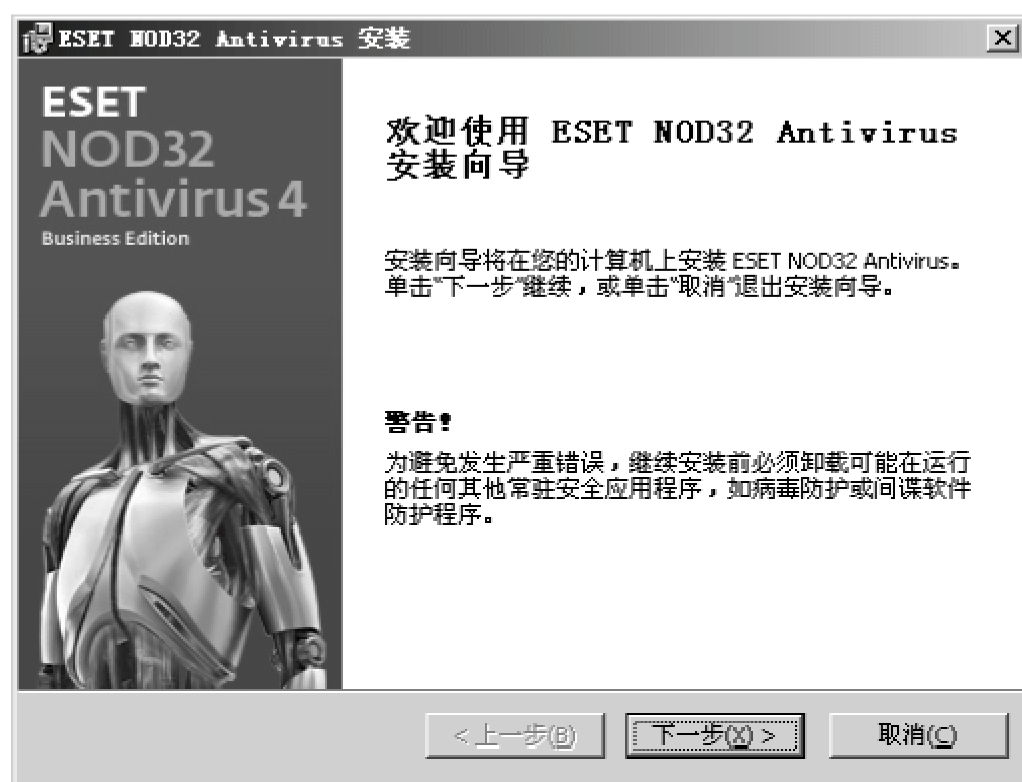


图 19-1　安装向导对话框

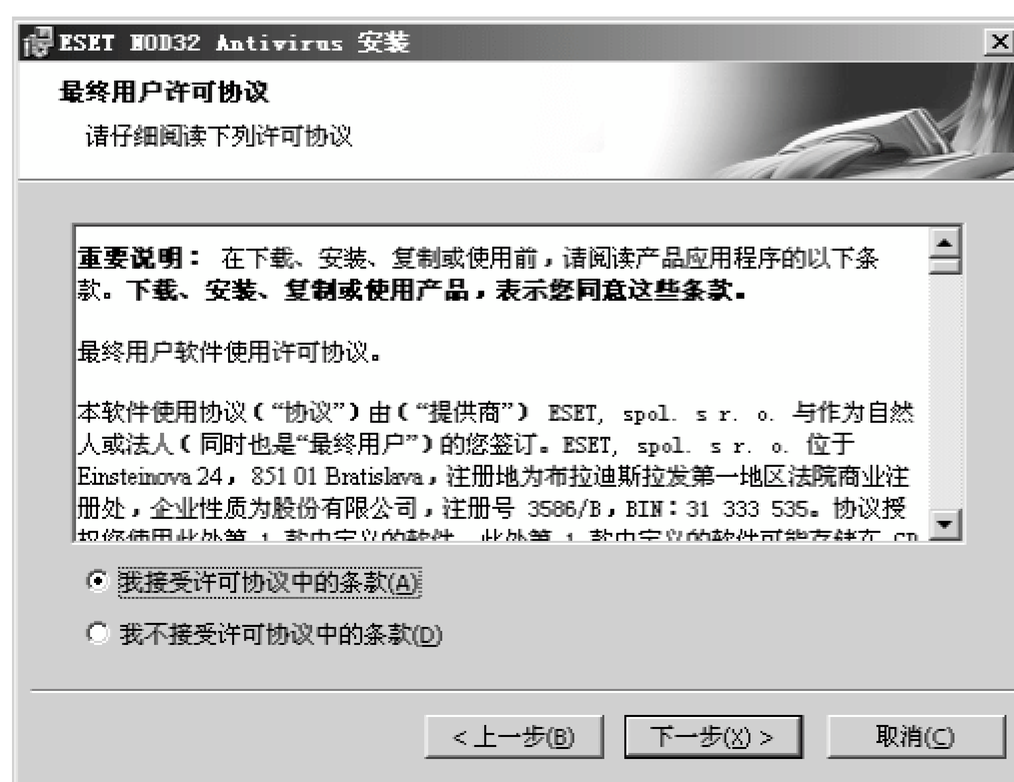


图 19-2　【最终用户许可协议】对话框

03 弹出【安装模式】对话框，根据个人情况选择安装模式，如果是初学者建议选择【典型】模式，单击【下一步】按钮，如图 19-3 所示。

04 弹出【自动更新】对话框，病毒软件需要及时更新程序及病毒库，在更新时需要向服务器提供有效的用户名及密码，在【用户名】和【密码】文本框分别输入已获得的用户名及密码信息。如果还没有用户名和密码，可选中【以后再设置用户名和密码】复选框。单击【下一步】按钮，如图 19-4 所示。



图 19-3　【安装模式】对话框



图 19-4　【自动更新】对话框

05 弹出【ThreatSense.Net 预警系统】对话框，通过该项配置可以及时提交系统遇到的最新威胁给 ESET 实验室，选中【启用 ThreatSense.Net 预警系统】复选框，并采用默认配置，单击【下一步】按钮，如图 19-5 所示。

06 弹出【检测潜在不受欢迎的应用程序】对话框，为了使计算机的性能、速度及可靠性更高，建议在下拉列表中选择【启用潜在不受欢迎的应用程序检测功能】选项，单击【下一步】按钮，如图 19-6 所示。



图 19-5 【ThreatSense.Net 预警系统】对话框



图 19-6 【检测潜在不受欢迎的应用程序】对话框

07 安装基本配置已经完成，弹出【准备安装】对话框，单击【安装】按钮，如图 19-7 所示。

08 系统自动安装程序并显示安装进度，可以单击【取消】按钮撤销本次安装，如图 19-8 所示。



图 19-7 【准备安装】对话框



图 19-8 自动安装对话框

09 安装结束，单击【完成】按钮，完成安装向导，如图 19-9 所示。

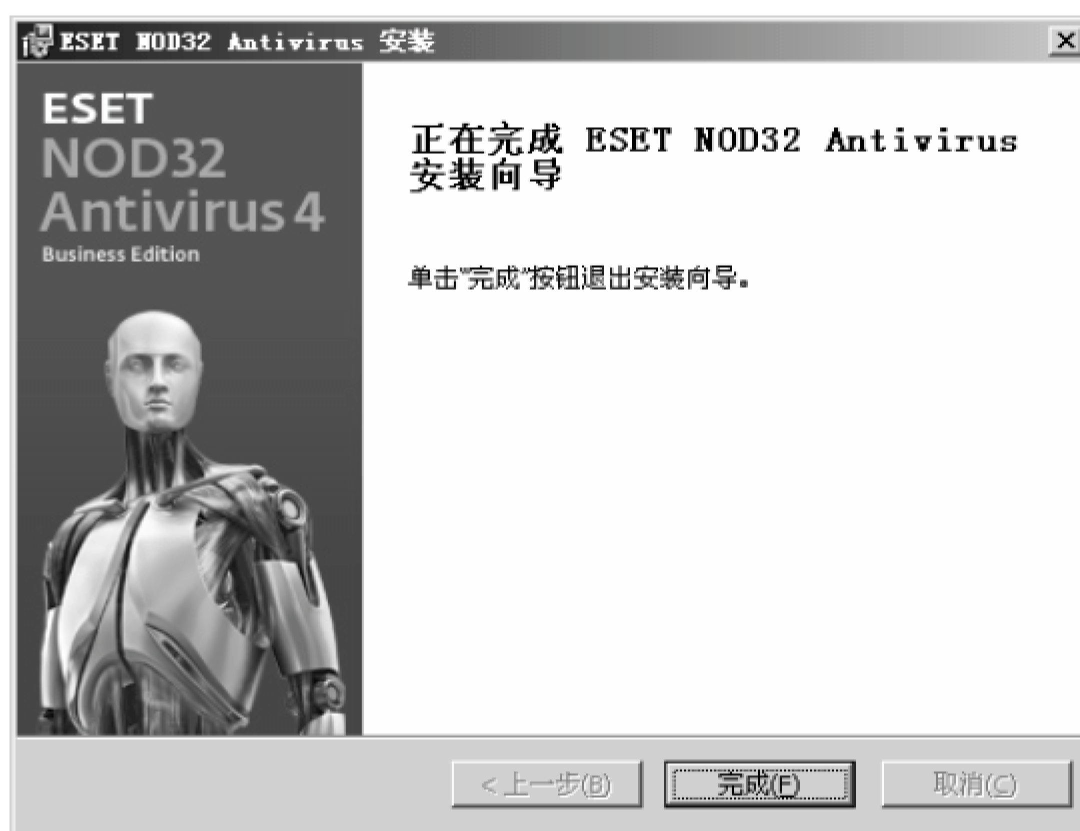


图 19-9 安装向导完成对话框

2. 安装远程管理服务器

ESET 远程管理服务器必须在指定的管理主机上安装，具体的安装步骤如下。

01 运行 ESET 远程管理服务器安装程序，弹出安装向导对话框，如图 19-10 所示，单击【下一步】按钮。

02 弹出【最终用户许可协议】对话框，选中【我接受许可协议中的条款】单选按钮，如图 19-11 所示，单击【下一步】按钮。



图 19-10 安装向导对话框

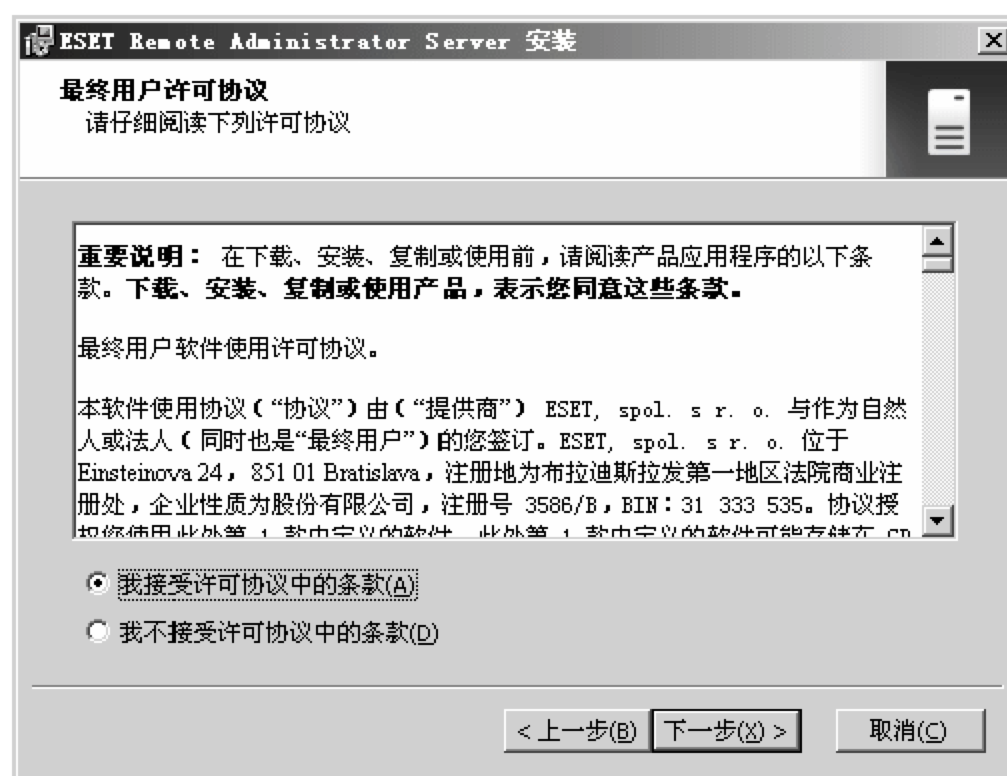


图 19-11 【最终用户许可协议】

03 弹出【选择安装类型】对话框，根据个人情况选择安装类型，如果是初学者建议选择【典型】模式，单击【下一步】按钮，如图 19-12 所示。

04 弹出【许可证密钥】对话框，单击【浏览】按钮选择已经获得的 lic 后缀的许可证密钥文件，添加成功后显示出该密钥支持的【产品】、【客户】及【到期时间】等信息，单击【下一步】按钮，如图 19-13 所示。



图 19-12 【选择安装类型】对话框

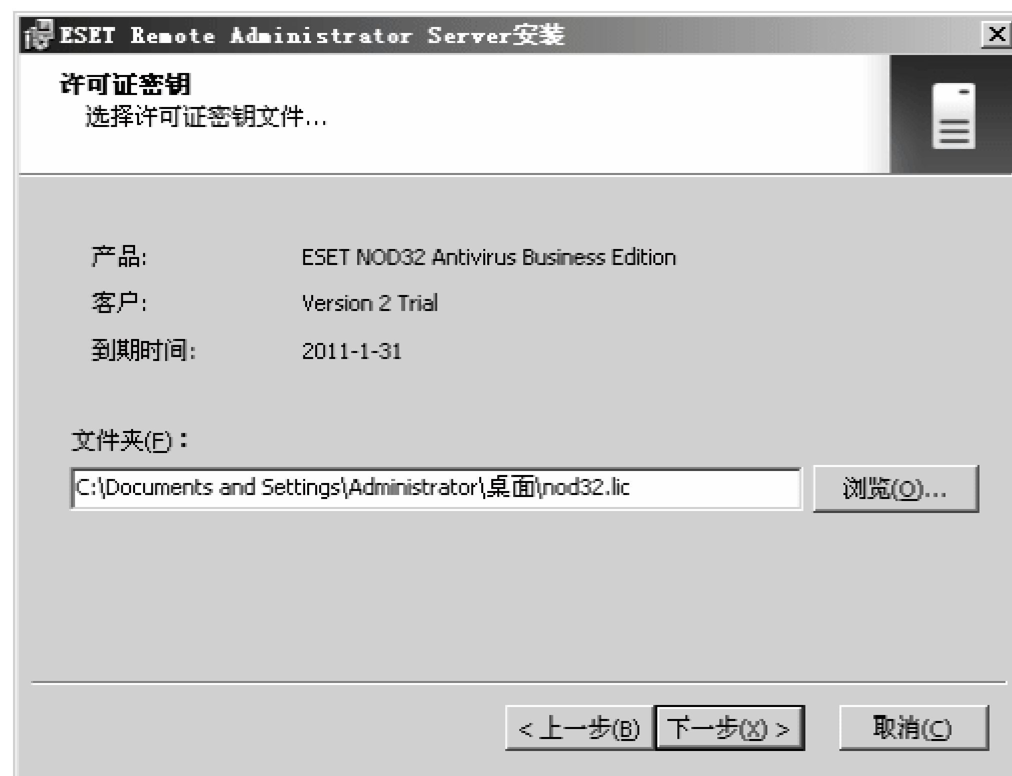


图 19-13 【许可证密钥】对话框

05 弹出【安全设置】对话框，单击【设置】按钮，可分别设置控制台管理员权限密码、控制台只读权限密码、远程代理安装程序密码、客户端密码、客户端和服务器同步密码，建议使用文档将密码妥善保管，配置完成后单击【下一步】按钮，如图 19-14 所示。

06 弹出【更新】对话框，选中【以后再设置更新参数】复选框，单击【下一步】按钮，如

图 19-15 所示。



图 19-14 【安全设置】对话框



图 19-15 【更新】对话框

07 安装基本配置已经完成，弹出【准备安装】对话框，单击【安装】按钮，如图 19-16 示。

08 系统自动安装程序，并显示安装进度可以单击【取消】按钮撤销本次安装，如图 19-17 所示。



图 19-16 【准备安装】对话框

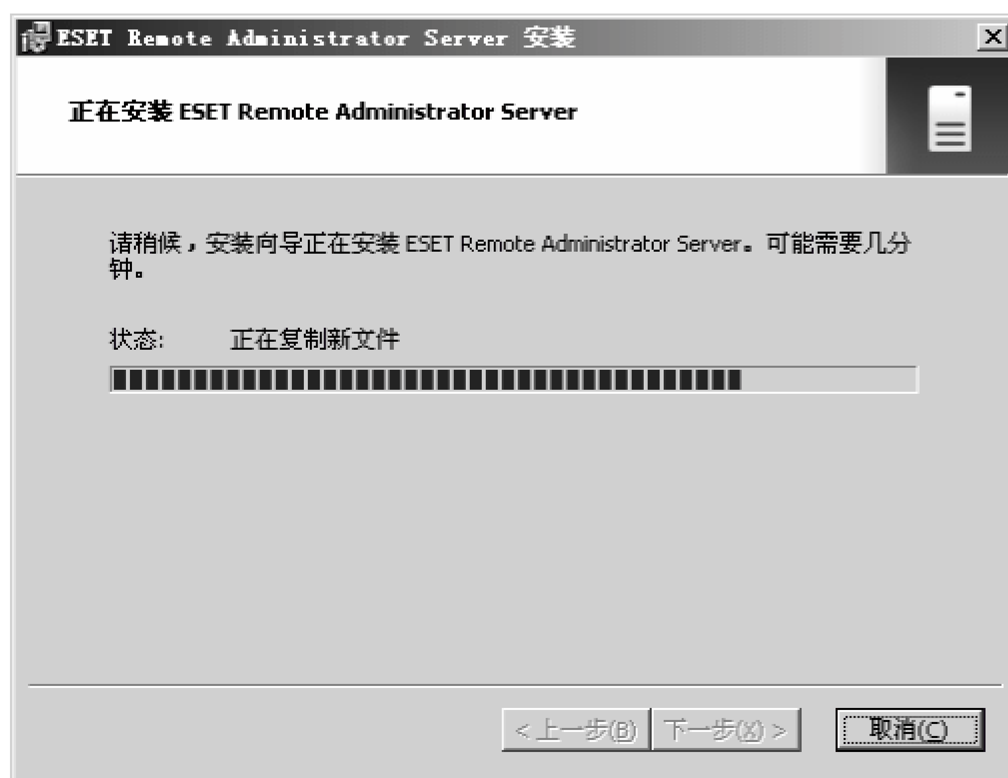


图 19-17 自动安装对话框

09 安装结束，单击【完成】按钮，完成安装向导，如图 19-18 所示。



图 19-18 完成安装向导对话框

3. 安装管理控制台

安装 ESET 管理控制台的主机要和安装 ESET 管理服务器的主机是同一台，其具体的安装步骤如下。

01 运行 ESET 管理控制台安装程序，弹出安装向导对话框，单击【下一步】按钮，如图 19-19 所示。

02 弹出【最终用户许可协议】对话框，选中【我接受许可协议中的条款】单选按钮，单击【下一步】按钮，如图 19-20 所示。



图 19-19　ESET 管理控制台安装向导对话框

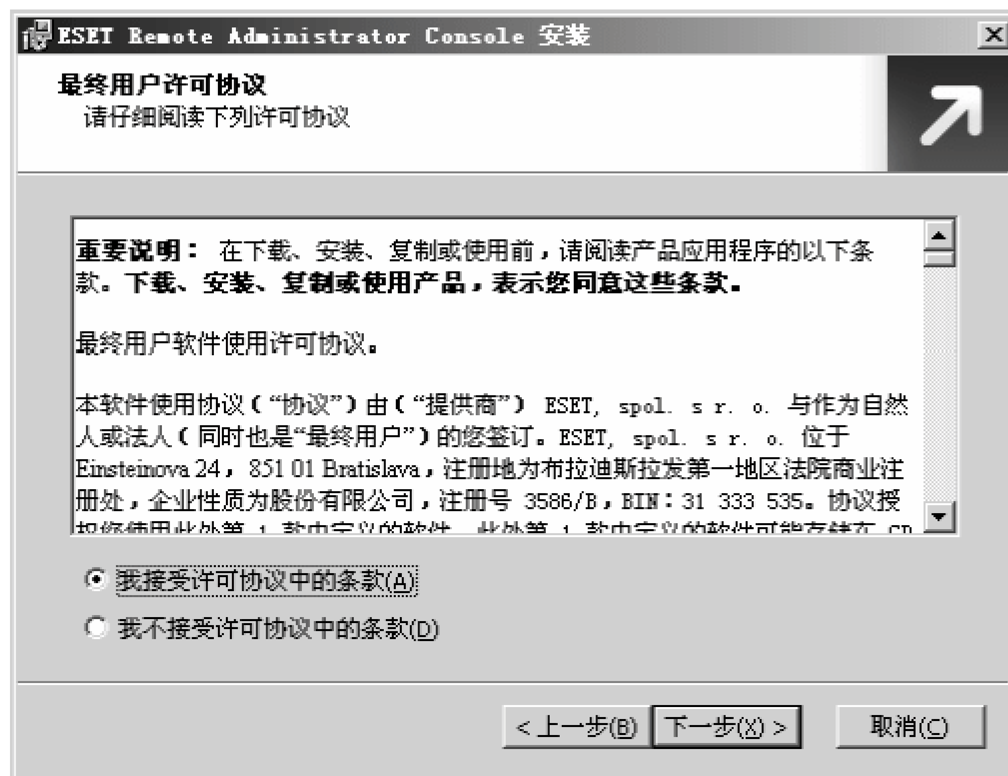


图 19-20　【最终用户许可协议】对话框

03 弹出【选择安装类型】对话框，根据个人情况选择安装类型，如果是初学者建议选择【典型】模式，单击【下一步】按钮，如图 19-21 所示。

04 弹出【选择安装文件夹】对话框，在【文件夹】文本框中输入程序安装目录，也可以单击【浏览】按钮指定安装目录，本实例采用默认配置，单击【下一步】按钮，如图 19-22 所示。

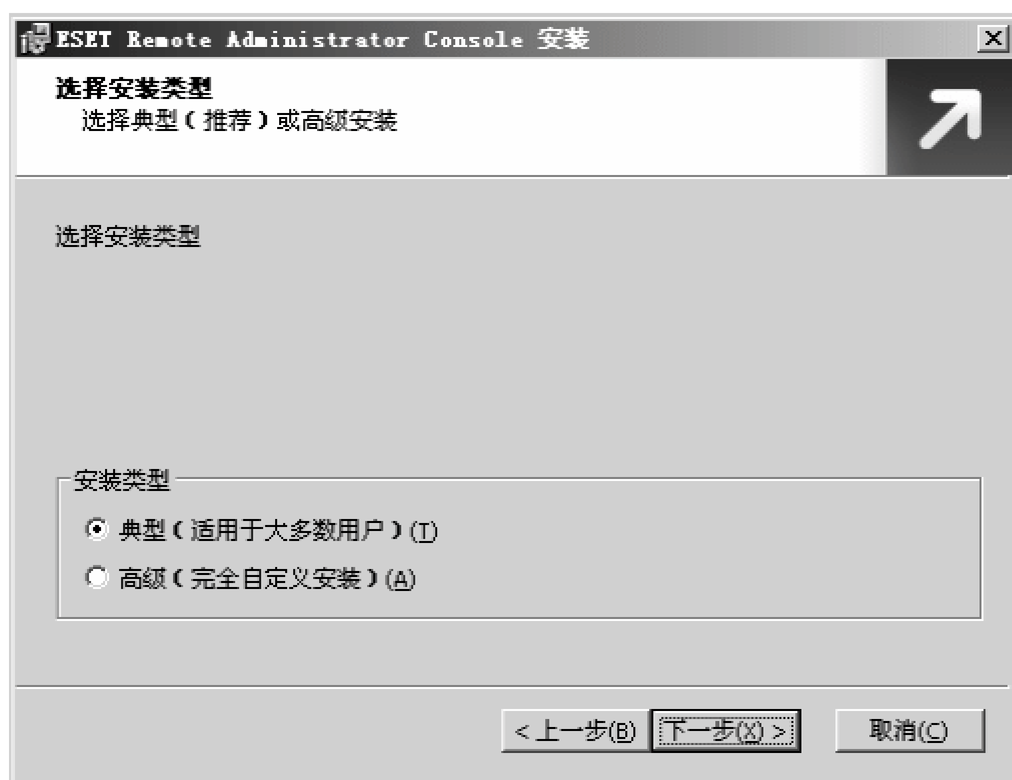


图 19-21　【选择安装类型】对话框

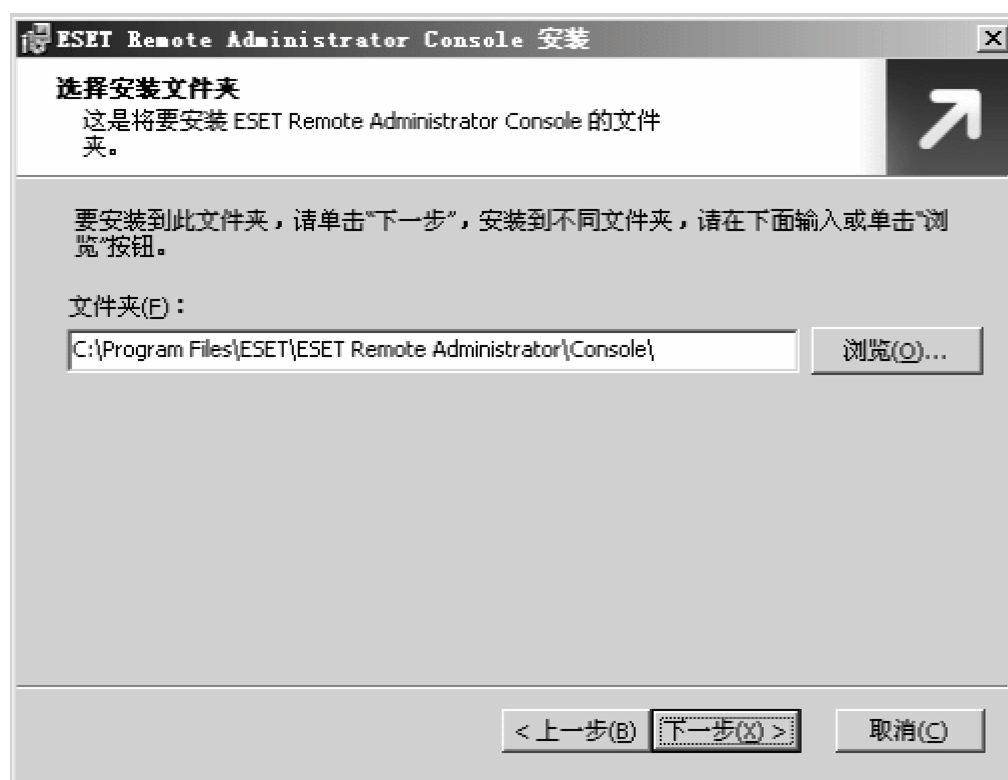


图 19-22　【选择安装文件夹】对话框

05 安装基本配置已经完成，弹出【准备安装】对话框，单击【安装】按钮，如图 19-23 所示。

06 系统自动安装程序，并显示安装进度，可以单击【取消】按钮撤销本次安装，如图 19-24 所示。



图 19-23 【准备安装】对话框

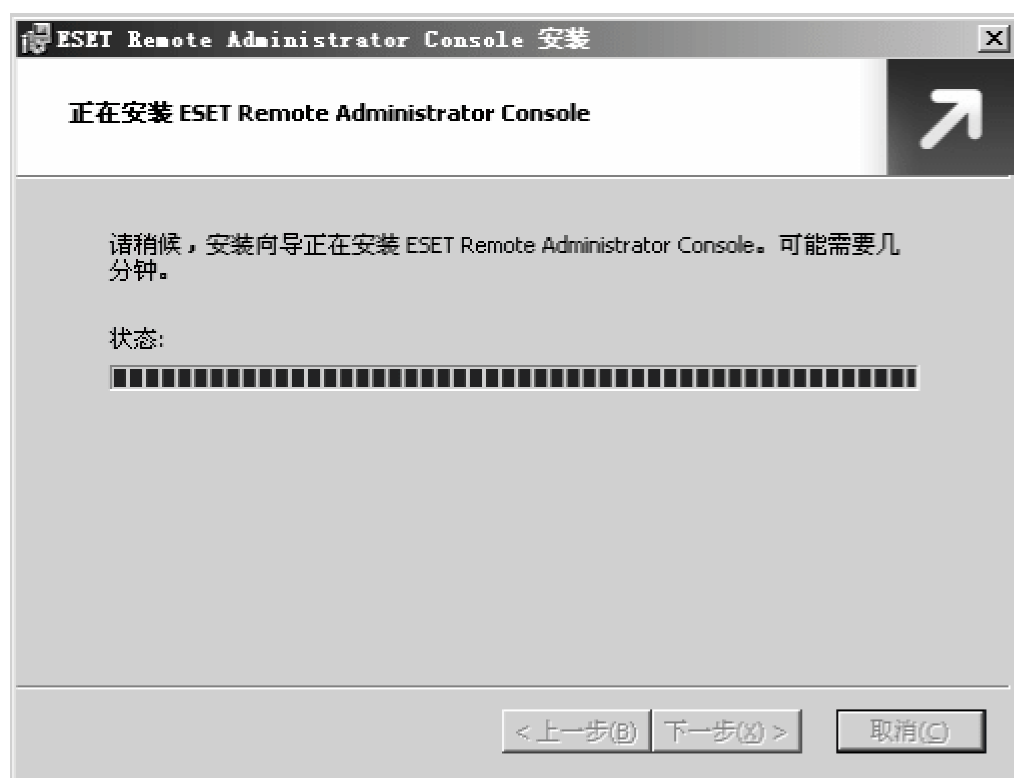


图 19-24 自动安装对话框

07 安装结束，单击【完成】按钮，完成安装向导，如图 19-25 所示。



图 19-25 完成安装向导对话框

19.2.2 设置 ESET 配置编辑器

在企业版中，需要通过管理控制台对所有反病毒客户机进行管理，管理控制台在使用之前需要先做基础管理配置，主要是对配置编辑器进行配置。通过配置编辑器可以更改客户端的配置，给客户端新增计划任务等。配置编辑器的配置内容比较多，本实例主要介绍两部分，分别是设置 ESET 内核和升级设置。

1. 打开配置编辑器

在设置 ESET 内核和升级之前，需要打开配置编辑器，具体的操作步骤如下。

01 双击桌面上的远程管理控制台程序 ESET Remote Administrator Console 的快捷方式，打开控制台程序主界面，弹出【输入服务器密码】对话框，【服务器】、【类型】和【访问权限】三项默认产生，只需要在【密码】文本框中输入安装程序时设置的密码即可，输入密码后单击【确定】按钮，如图 19-26 所示。

02 密码验证成功后，选择【工具】➢【ESET 配置编辑器】选项，如图 19-27 所示。

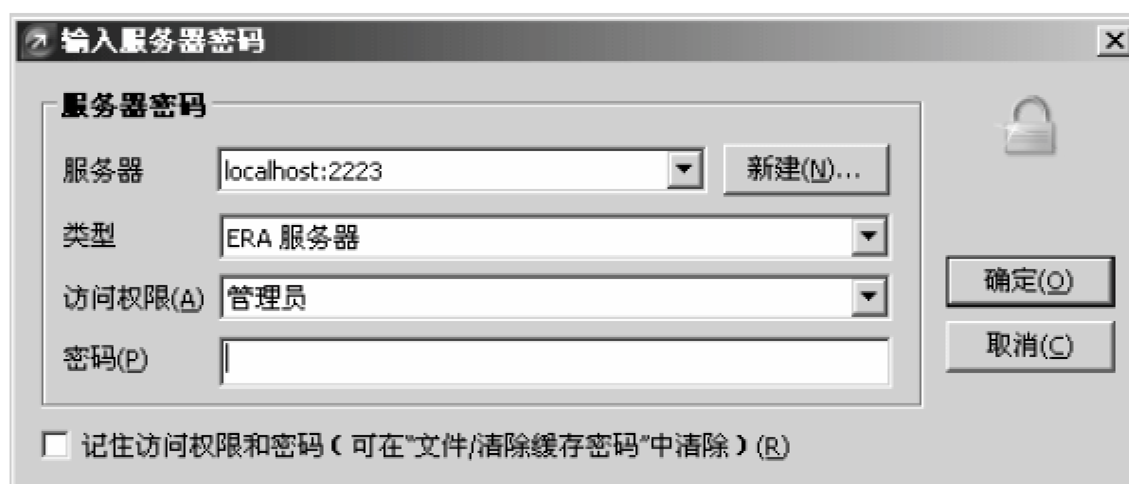


图 19-26　【输入服务器密码】对话框



图 19-27　ESET 配置编辑器选项

03 弹出【ESET 配置编辑器】窗口。配置编辑器左侧以树状结构显示配置内容，大部分的配置都在 ESET Smart Security,ESET NOD32 Antivirus 里，所以本实例只对这部分进行配置，如图 19-28 所示。



图 19-28　【ESET 配置编辑器】窗口

2. 设置 ESET 内核

在 ESET 内核配置中，主要配置以下三项内容。

1）远程管理配置

远程管理用于指定工作站要连接的远程管理服务器的地址，具体的配置步骤如下。

01 选择【ESET 内核】➢【设置】➢【远程管理】选项，显示出【远程管理】配置项的内置内容，如图 19-29 所示。



图 19-29 【远程管理】配置项

02 选择【连接到 Remote Administrator Server】选项，在右侧选中【值】复选框，使管理控制台连接到管理服务器，如图 19-30 所示。



图 19-30 【连接到 Remote Administrator Server】选项

03 选择【主服务器地址】选项，在右侧【值】文本框中输入客户机需要连接的服务器 IP 地址，本实例采用“192.168.1.102”，如图 19-31 所示。



图 19-31 【主服务器地址】选项



提 示

【远程管理】中的其他选项可以根据实际情况配置，其中【主服务器端口】的值是客户端连接到远程管理服务器的默认端口，如果在远程管理服务器上安装了防火墙，需要设定防火墙允许该端口流量通信，否则客户端是连接不上的。

2）设置保护参数

可以设置保护密码，客户端获得保护密码后可以起到保护作用，防止客户端配置被随意更改或者客户端被卸载等。

设置保护参数的具体操作步骤如下。

01 选择【ESET 内核】➢【设置】➢【保护设置参数】➢【要解除锁定的密码】选项，单击右侧【设置密码】按钮，如图 19-32 所示。

02 弹出【密码】对话框，在【输入密码】和【确认密码】文本框中输入具有较高安全性的密码，不可使用如“123456”一样的简单密码，单击【确定】按钮，如图 19-33 所示。





图 19-32 【要解除锁定的密码】选项　　图 19-33 【密码】对话框

03 设置密码成功，在【要解除锁定的密码】后出现密码字符串“******”，如图 19-34 所示。



图 19-34 成功设置【要解除锁定的密码】

3）计划任务

管理员不可能时刻在管理控制台面前管理客户机，对于一些常规管理任务，应尽量由服务器自己完成，同时企业员工的计算机水平差异很大，管理员应定期对所有客户机进行病毒查杀。考虑这些需求，制作计划任务显得很重要，制作好的计划任务会自动分发到所有客户机。

制作计划任务的具体操作步骤如下。

01 选择【ESET 内核】➢【设置】➢【计划任务】➢【计划任务】选项，单击右侧【编辑】按钮，如图 19-35 所示。

02 弹出【计划任务】对话框，单击【添加】按钮，如图 19-36 所示。



图 19-35 【计划任务】选项

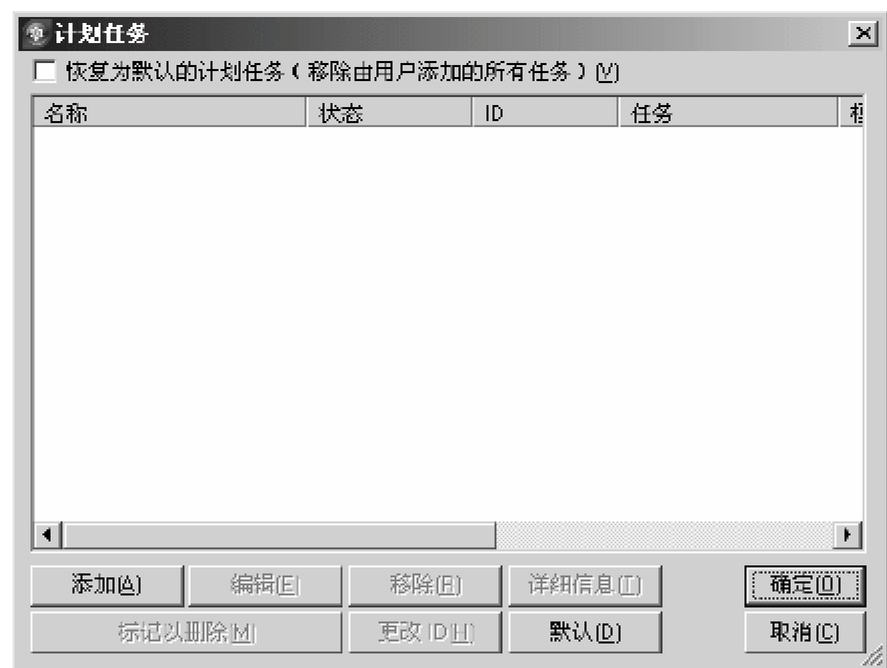


图 19-36 【计划任务】对话框

03 弹出【添加任务】对话框，在【计划的任务】下拉列表中可以选择要执行的任务类型，如图 19-37 所示。

该下拉列表中各项的参数含义如下。

- 【运行外部应用程序】：可以让客户端按照计划运行其他外部程序，这个功能使用比较少。
- 【日志维护】：定期进行日志维护，特别是大型企业，新日志产生的速度很快，如果长期不清理，会占用很多空间。

- 【计算机扫描】：定时扫描计算机，并按照要求查杀病毒。
- 【创建计算机状态快照】：可按照计划对计算机状态进行周期性快照记录。
- 【更新】：定时更新病毒库，默认情况下 ESET NOD32 会每小时自动更新病毒库，所以此功能可以不用设置。
- 【自动启动文件检查】：计算机启动时，自动扫描启动文件，防止病毒在计算机启动时运行，并查杀启动文件夹中的病毒。

04 在【计划的任务】下拉列表框中选择【计算机扫描】选项，每周进行一次计算机扫描，单击【下一步】按钮，如图 19-38 所示。

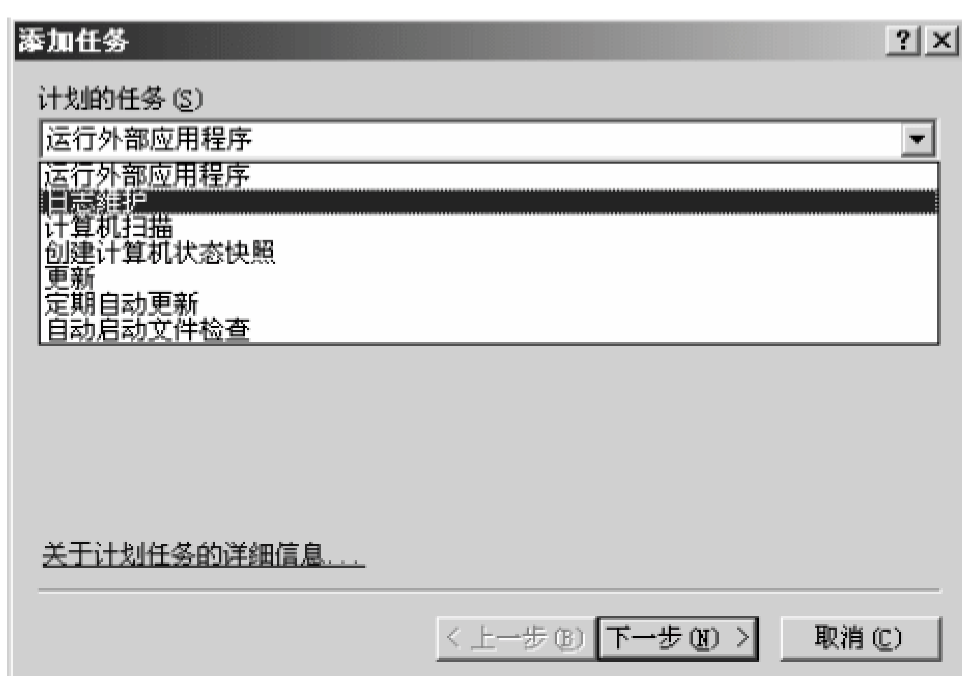


图 19-37 【添加任务】对话框



图 19-38 选择【计算机扫描】选项

05 在弹出的对话框的【任务名称】文本框中输入本次计划任务的名称，本实例输入“每周扫描”，并在【执行任务】选项组中选中【每周】单选按钮，单击【下一步】按钮，如图 19-39 所示。

06 在弹出的对话框的【任务执行时间】文本框中指定时间为“8:00:00”，选中【周一】复选框，每周一早晨 8 点执行任务，单击【下一步】按钮，如图 19-40 所示。

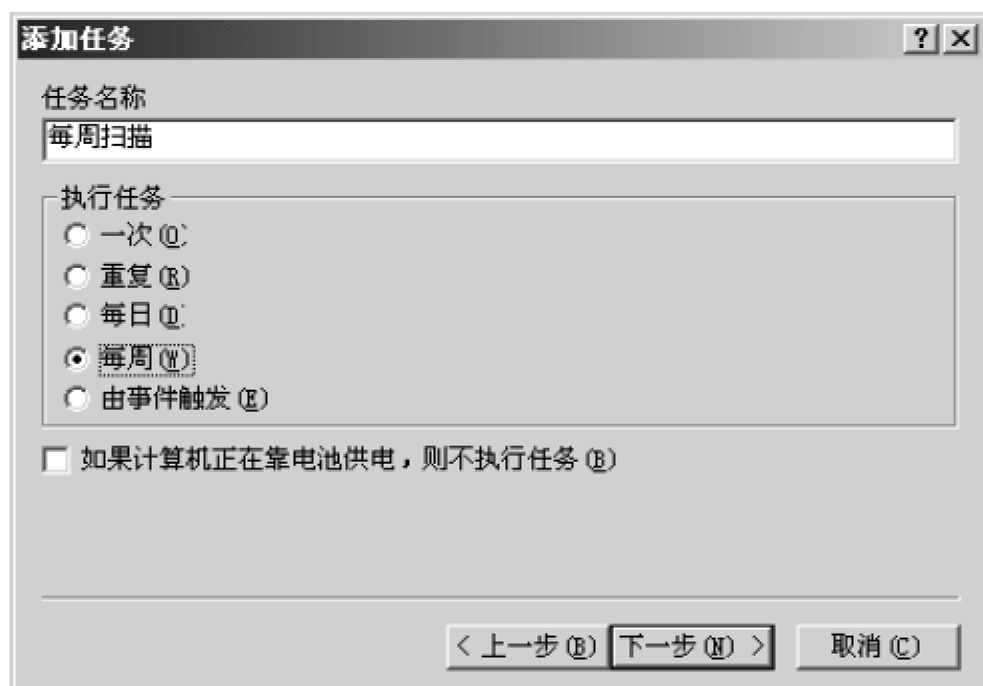


图 19-39 设置任务名称及频率

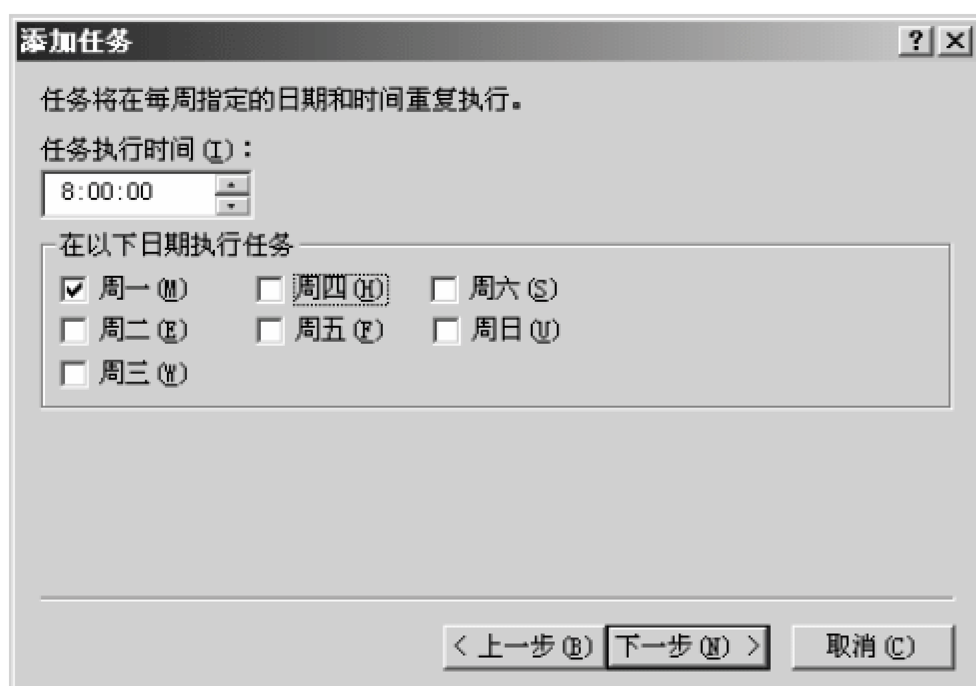


图 19-40 设置任务执行时间

07 如果在预定的任务计划时间内系统由于关机等原因无法完成任务，应让系统在恢复正常后迅速执行计划任务，选中【尽快执行任务】单选按钮，单击【下一步】按钮，如图 19-41 所示。

08 计划任务配置完成，在弹出的对话框中显示了计划任务的详细配置，单击【完成】按钮，如图 19-42 所示。

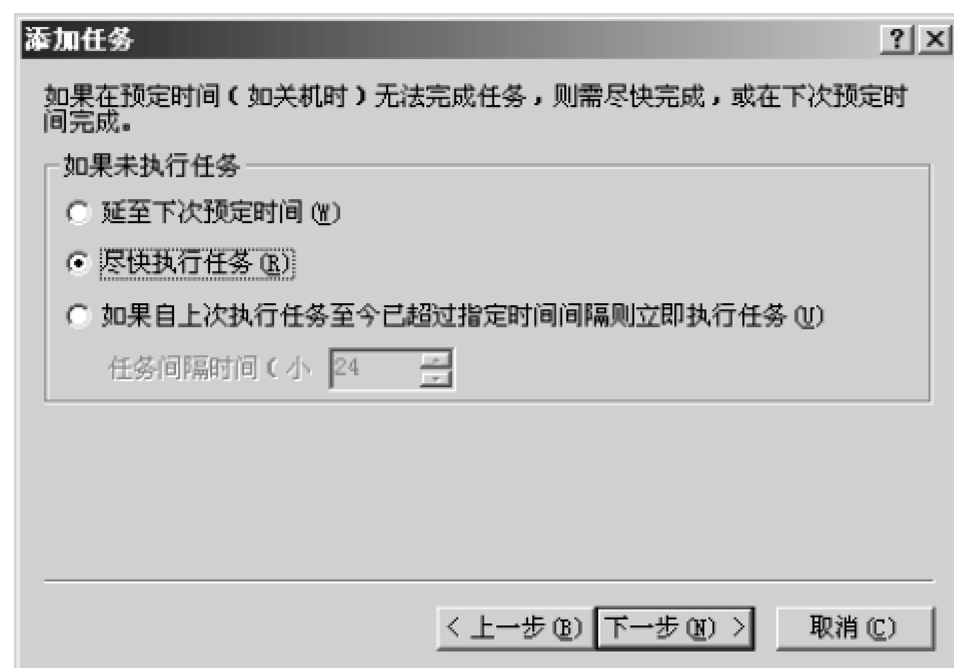


图 19-41 设定未完成任务的操作

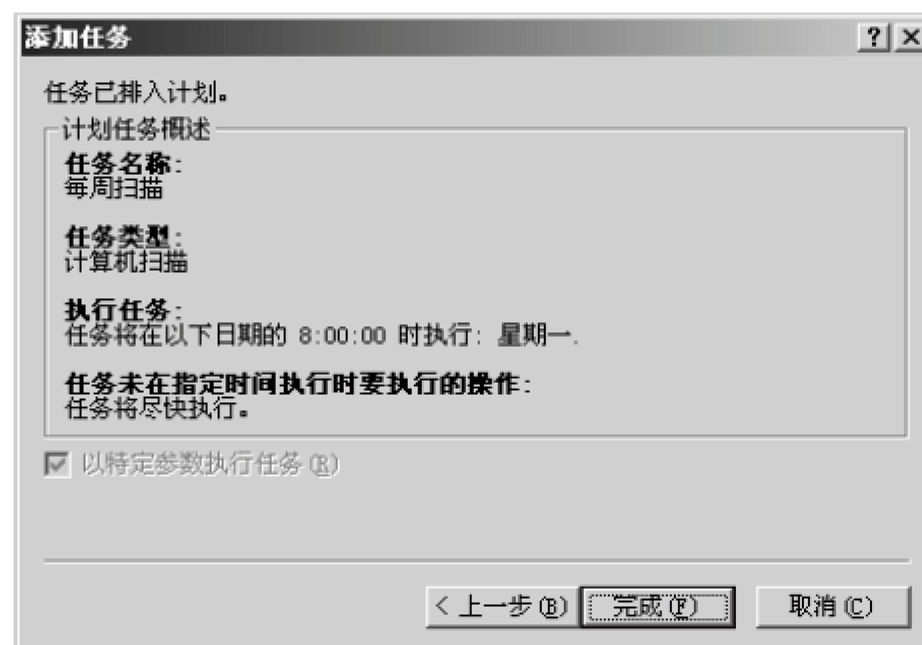


图 19-42 计划任务的详细配置

09 弹出【特殊设置】对话框，在【说明】文本框中输入关于本次计划任务的描述“每周扫描计算机”，选择【配置文件】选项，在【值】下拉列表框中选择计算机扫描采用的配置文件，本实例采用默认配置“全面扫描”，如图 19-43 所示。

10 选择【目标】选项，单击【目标】按钮，指定扫描目标，如图 19-44 所示。

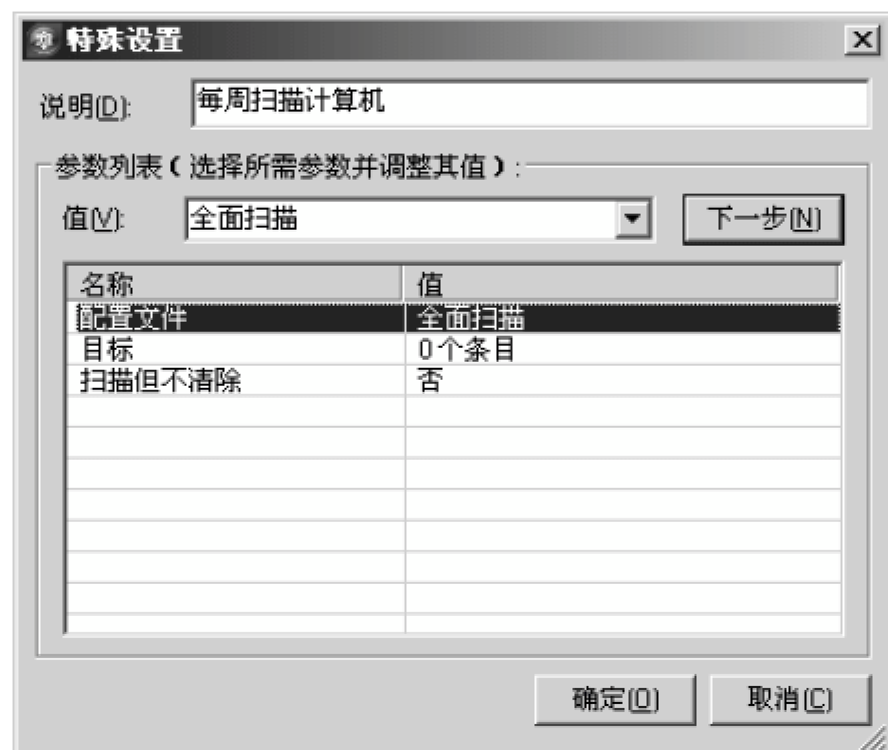


图 19-43 【特殊设置】对话框



图 19-44 设定扫描目标

11 弹出【文件夹和文件】对话框，可以指定文件夹、文件、列表、驱动器和内存为扫描目标，本实例以驱动器为例进行介绍，单击【驱动器】按钮，如图 19-45 所示。

12 弹出【客户端扫描目标选择】对话框，可根据情况进行选择，为了安全建议选中【所有驱动器】复选框，单击【确定】按钮，如图 19-46 所示。

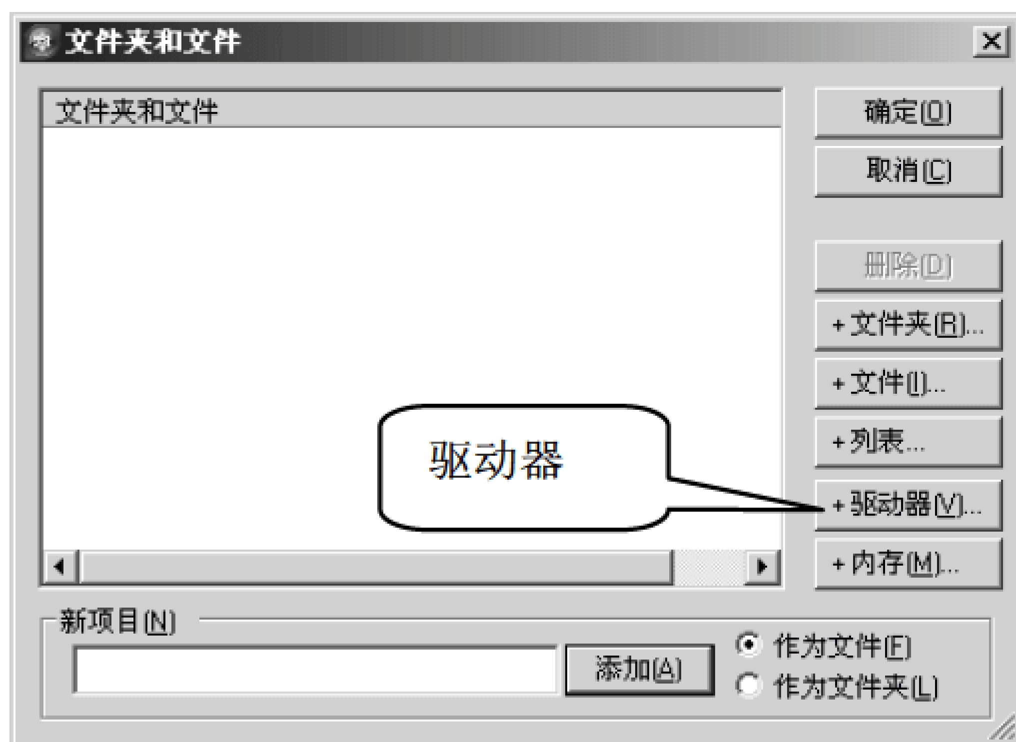


图 19-45 【文件夹和文件】对话框



图 19-46 【客户端扫描目标选择】对话框

13 返回【文件夹和文件】对话框，可继续添加其他目标，单击【确定】按钮，完成添加，如图 19-47 所示。

14 返回【特殊设置】对话框，【目标】选项后的【值】显示为【1 个条目】，单击【确定】按钮，如图 19-48 所示。



图 19-47　扫描目标添加完成



图 19-48　【特殊设置】对话框

15 返回【计划任务】对话框，计划任务添加成功，并自动分配了任务 ID，可以单击【添加】按钮继续添加计划任务，添加完成后单击【确定】按钮，如图 19-49 所示。

16 返回【ESET 配置编辑器】窗口，可以看到“计划任务：总计 1/0”，表示当前已有有一个计划任务添加成功，如图 19-50 所示。

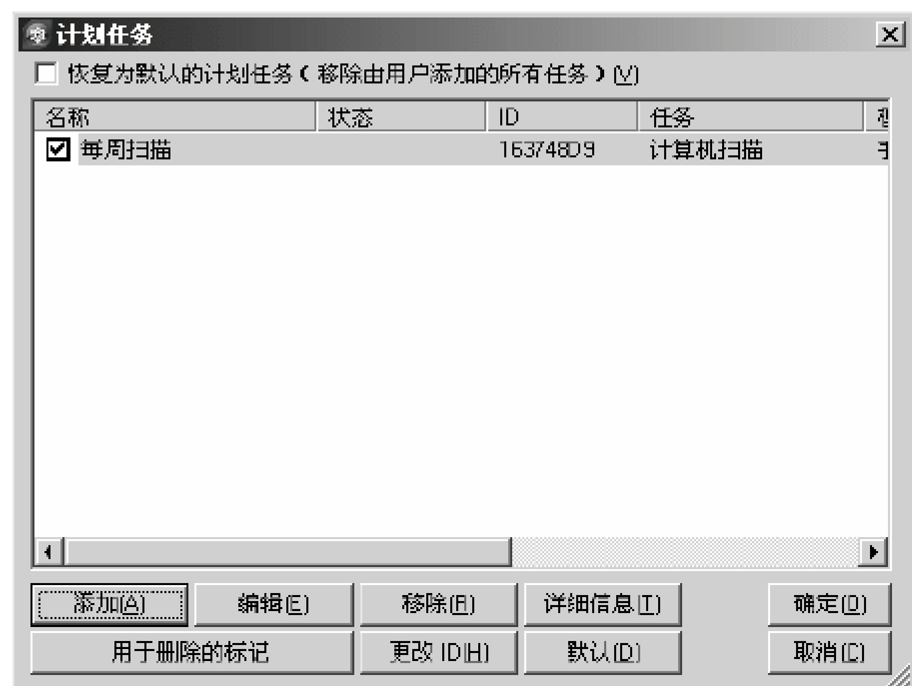


图 19-49　计划任务添加完成

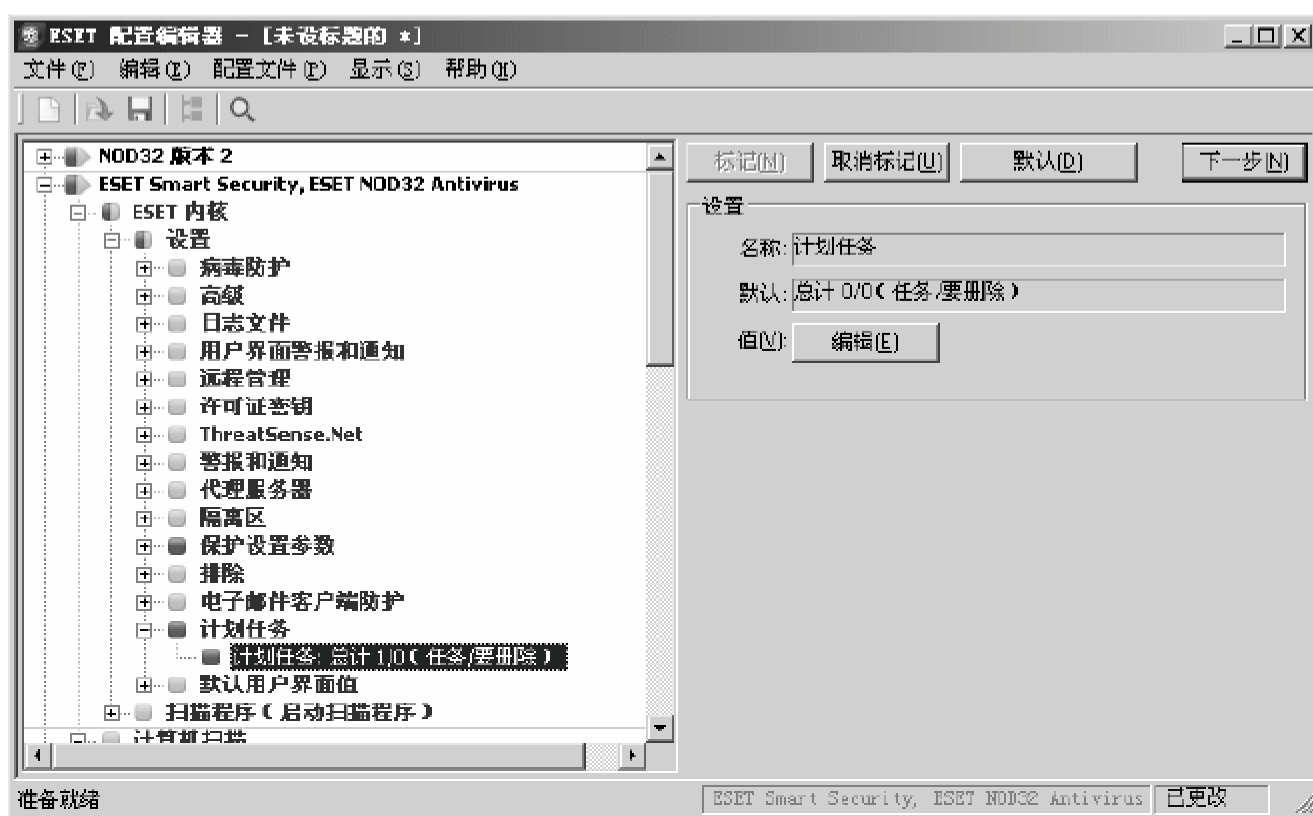


图 19-50　【ESET 配置编辑器】窗口

3. 更新模块的设置

所有客户机在更新程序及病毒库时，必须要有统一的更新配置，其中最重要的就是更新服务器的配置。下面介绍更新模块的配置方法。

选择【更新模块】➢【配置文件】➢【设置】➢【更新服务器】选项，在右侧【值】文本框中输入客户机可用的更新服务器地址，一般为安装 ESET 管理服务器的主机，本实例采用“http://192.168.1.102:2221”，如图 19-51 所示。其他【设置】项可根据情况配置。



图 19-51 更新模块设置内容

4. 保存配置编辑器

配置编辑器设置完成后，要妥善保存。保存配置的具体步骤如下。

01 单击【ESET 配置编辑器】工具栏的按钮，弹出 CfgEdit 对话框，单击【是】按钮。

02 弹出【另存为】对话框，在【保存在】下拉列表框中选择合适的保存目录“我的文档”，在【文件名】文本框中输入保存的文件名“config”，在【保存类型】下拉列表框中选择【配置文件（*.xml）】选项，单击【保存】按钮。



图 19-52 配置编辑器保存提示框

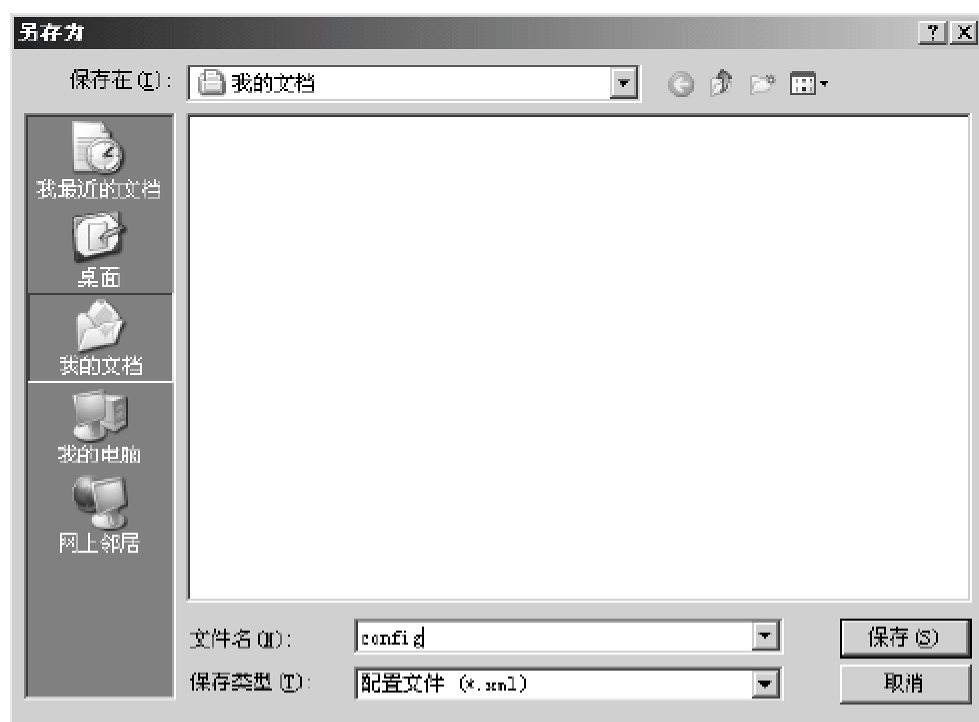


图 19-53 【另存为】对话框



配置编辑器的其他内容，基本上都可以不用去修改，系统已经默认设定好大部分的参数，这些默认配置可以最大限度地平衡计算机的性能。

19.2.3 设置客户端连接

客户端安装之后，需要被控制台统一管理，这需要在所有客户端配置连接管理控制服务器。设置客户端连接的具体操作步骤如下。

01 运行 ESET NOD32 客户端反病毒程序，打开程序主界面，选择左侧的【设置】选项，单

击右侧的【切换到高级模式】超级链接，如图 19-54 所示。

02 弹出【切换到高级模式】对话框，单击【是】按钮，如图 19-55 所示。



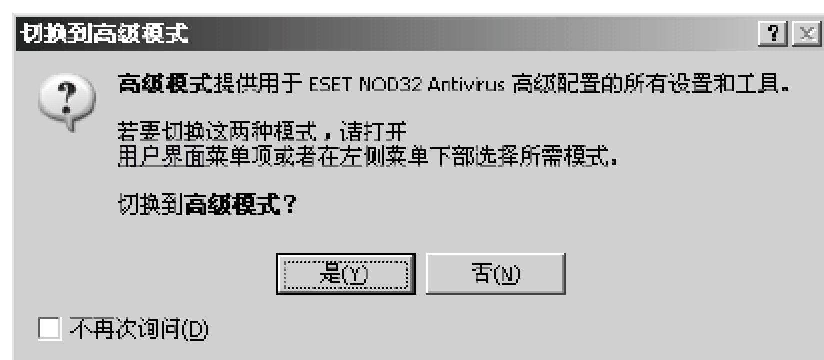


图 19-54　ESET NOD32 反病毒程序客户端窗口　　图 19-55　【切换到高级模式】提示框

03 在主界面的右下方显示了更多配置项，单击【显示所有高级设置】超级链接，如图 19-56 所示。

04 弹出【设置】对话框，在左侧选择【更新】选项，在右侧【更新服务器】下拉列表框中选择更新程序及病毒库的服务器，默认使用【自动选择】，也可以单击【编辑】按钮进行添加，如图 19-57 所示。



图 19-56　选择显示所有高级设置

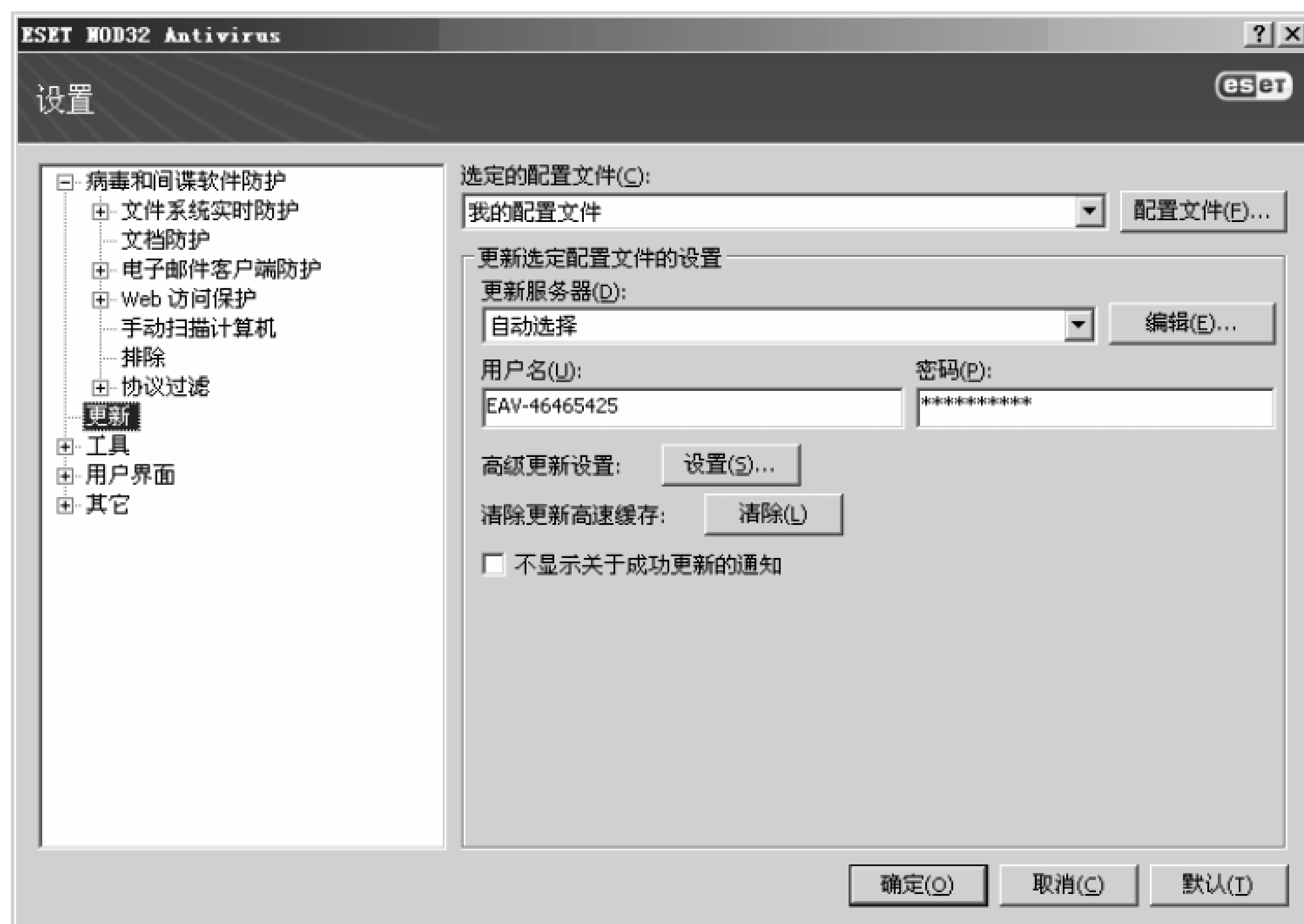


图 19-57　ESET NOD32【设置】对话框

05 弹出【更新服务器列表】对话框，在【更新服务器】文本框中输入客户端可使用的更新服务器地址，该地址在管理服务器端有设置，本实例采用的是“http://192.168.1.102:2221”，单击【添加】按钮，如图 19-58 所示。

06 添加成功，在【更新服务器列表】列表框中有添加后的地址，可以双击服务器地址直接修改，更新服务器地址正确添加后，单击【确定】按钮，如图 19-59 所示。



图 19-58　【更新服务器列表】对话框



图 19-59　更新服务器列表

07 返回【设置】对话框，【更新服务器】下拉列表框中的地址已经制定成功，如图 19-60 所示。

08 在左侧选项中选择【其他】➢【远程管理】选项，在右侧【服务器地址】文本框中输入安装管理服务器程序的主机 IP 地址，本实例采用“192.168.1.102”，在【端口】文本框中输入管理服务器指定的“2222”端口，单击【确定】按钮，完成客户端的配置，如图 19-61 所示。

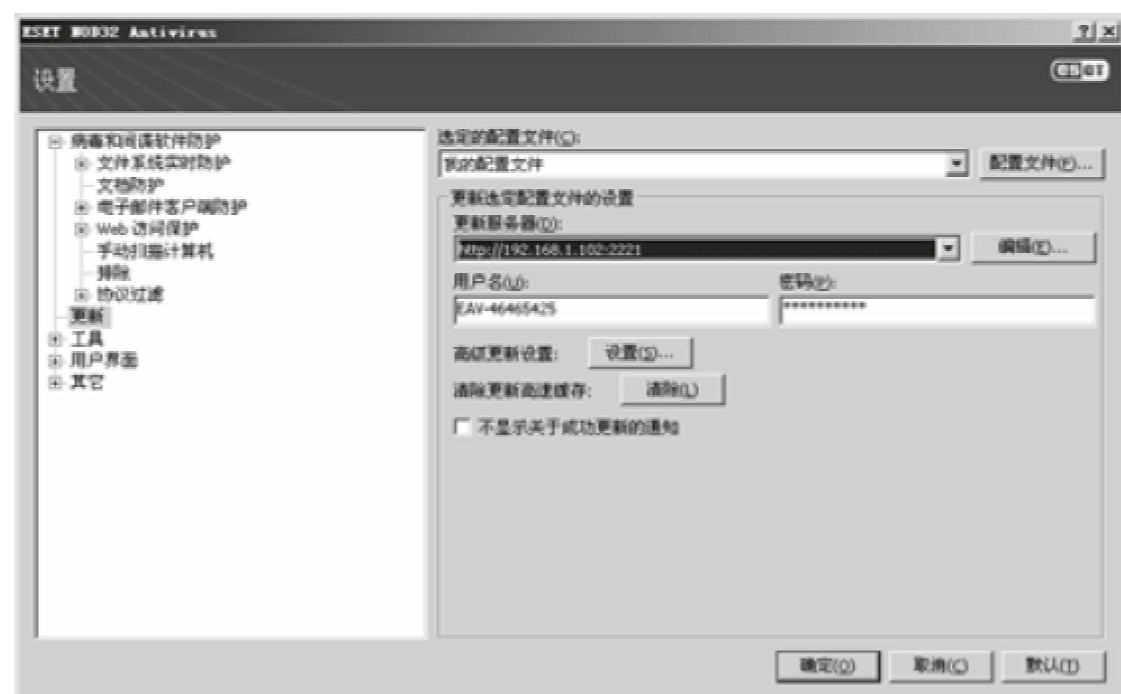


图 19-60　更新服务器地址配置成功

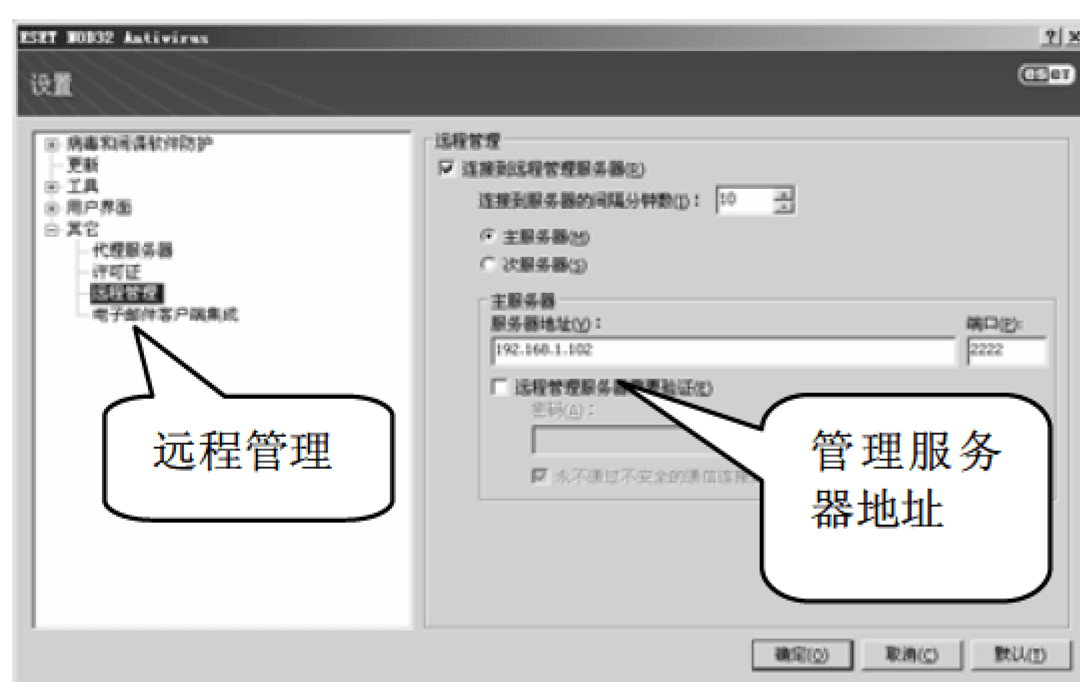


图 19-61　配置远程管理服务器地址

19.2.4　使用 ESET NOD32 进行全网杀毒

企业反病毒系统的环境做好之后，在日常管理中经常会遇到客户端感染病毒的现象发生，对此需要控制台对单个主机或全网进行病毒查杀。

在控制台进行全网病毒监控及查杀的具体操作步骤如下。

01 选择已有客户端，右击鼠标，在弹出的快捷菜单中选择【新任务】➢【手动扫描】命令，如图 19-62 所示。

在【新任务】选项后有多个选项，主要选项介绍如下。

- 【配置任务】：用于配置计划任务，可不在此配置。
- 【手动扫描】：有两个选项，其差异在于扫描到病毒后的操作，【清除已禁用】表示对扫描到的病毒只做提示但不清除，而【清除已启用】会将扫描到的病毒直接清除。
- 【立即更新】：从图 19-26 中可以看出，上方【病毒库状态】选项下有红色提示"某些较旧"，可以选择【立即更新】选项解决病毒库或反病毒程序较旧的问题。

02 弹出【手动扫描】窗口，【配置部分】和【配置文件名】按默认配置，在【要扫描的驱动】列表框中，选择需要扫描的项目，本实例采用默认配置，左下角的【扫描但不清除】复选框可根据情况选择，单击【下一步】按钮，如图 19-63 所示。



图 19-62　执行手动扫描功能



图 19-63　【手动扫描】窗口

03 弹出【选择客户端】窗口，通过双击或者拖放的形式将左侧【所有项】列表中的服务器或客户端放入右侧【选定项目】列表中，单击【下一步】按钮，如图 19-64 所示。

04 弹出【任务报告】窗口，在【新任务的最终报告】列表框中显示新建扫描任务，在【任务设置】选项域的【名称】文本框中输入本次任务名，可以通过选中【该时间之后应用任务】复选框，设定定时扫描计划，本实例不作操作，为了方便排查故障，不建议选中【如果成功完成，则通过清除功能自动删除任务】复选框，单击【完成】按钮，开始客户端扫描，如图 19-65 所示。

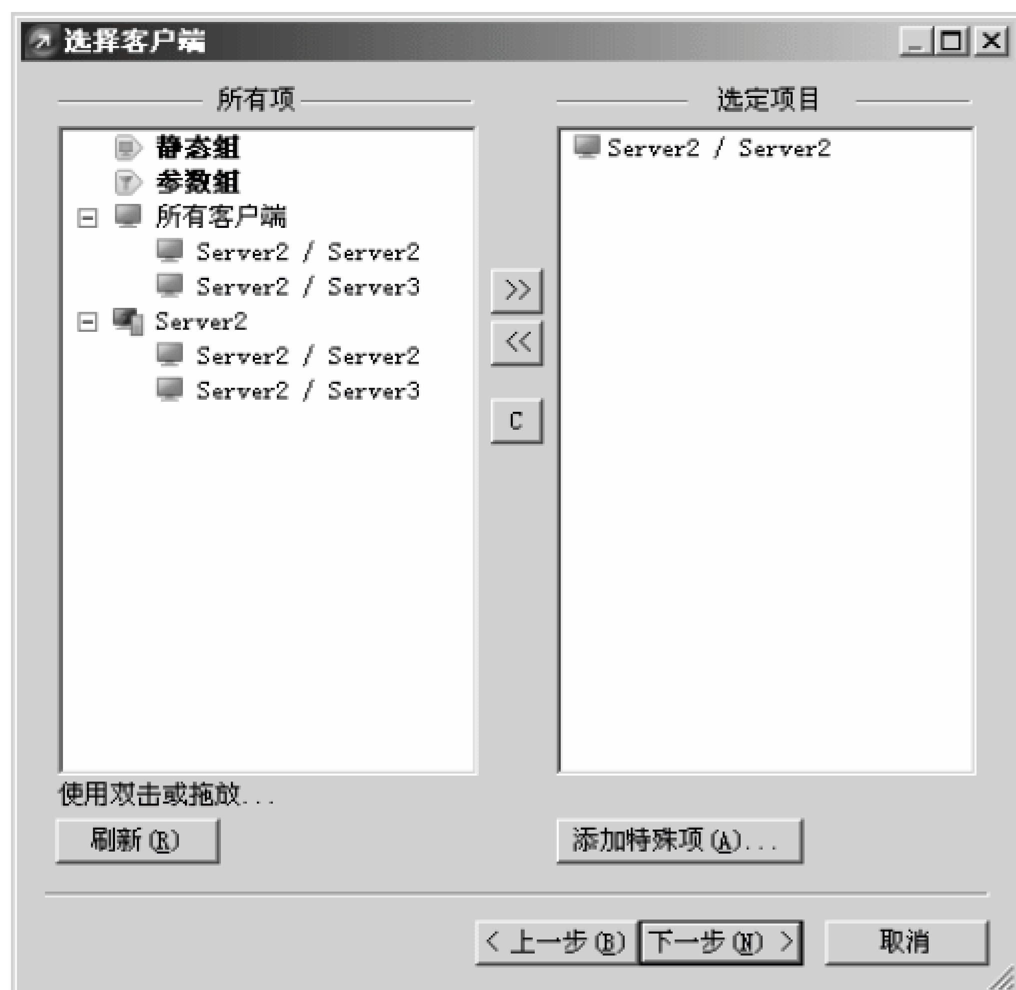


图 19-64 【选择客户端】窗口



图 19-65 【任务报告】窗口

19.3 项目实战 2：趋势科技企业反病毒系统实战案例

趋势科技是国内实力很强的反病毒系统，对于中国式病毒的防护具有比较显著的优势，下面详细介绍其环境架设及应用。

19.3.1 安装趋势科技企业反病毒系统

趋势科技反病毒系统对计算机内存要求稍高，最好使用 1G 以上内存。安装趋势科技反病毒系统的具体操作步骤如下。

01 运行趋势科技防毒墙网络版安装程序，弹出安装向导，单击【下一步】按钮，如图 19-66 所示。

02 弹出【许可证协议】对话框，选中【我接受许可证协议中的条款】单选按钮，单击【下一步】按钮，如图 19-67 所示。

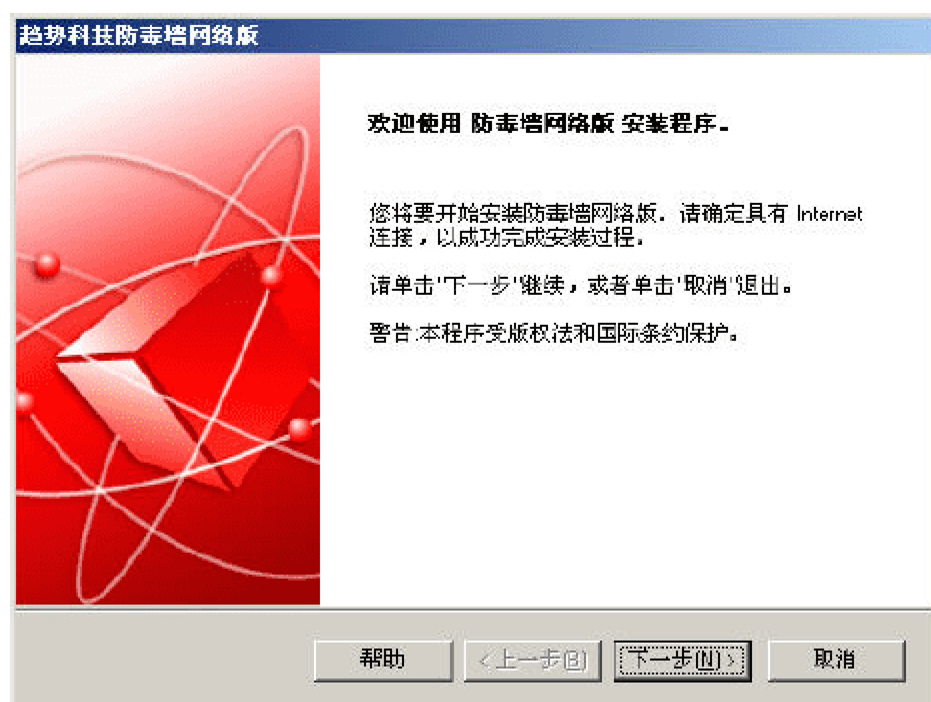


图 19-66　趋势科技防毒墙网络版安装向导

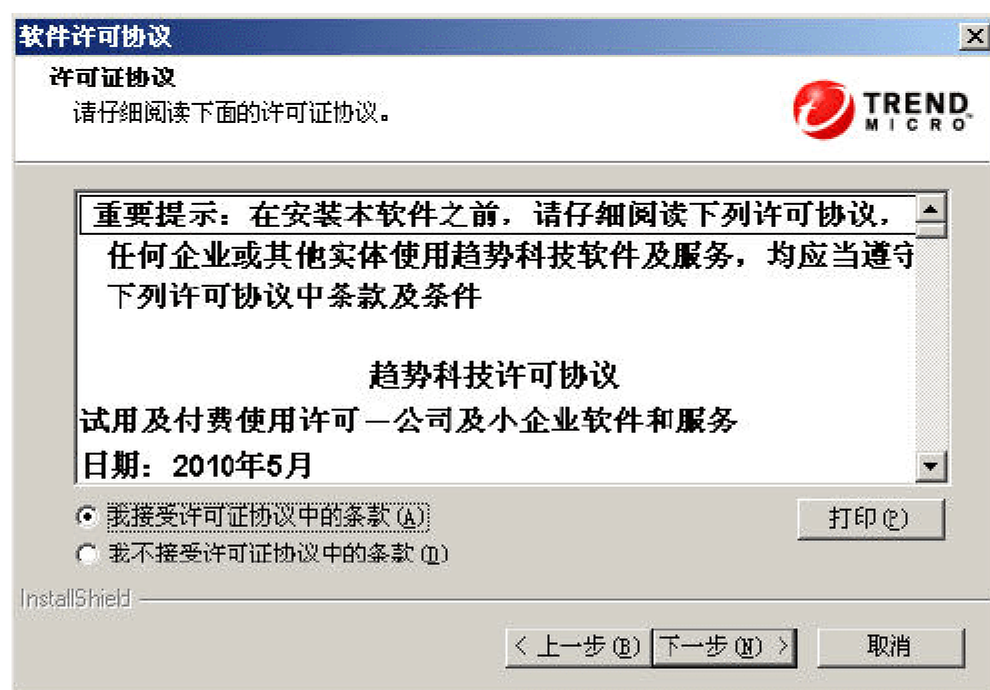


图 19-67　【许可证协议】对话框

03 弹出【客户端部署】对话框，给出将客户端安装软件包部署到防毒墙网络版客户端所需的预估网络带宽，单击【下一步】按钮，如图 19-68 所示。

04 弹出【使用指南】对话框，提示安装前备份现有服务器配置，默认不操作，单击【下一步】按钮，如图 19-69 所示。

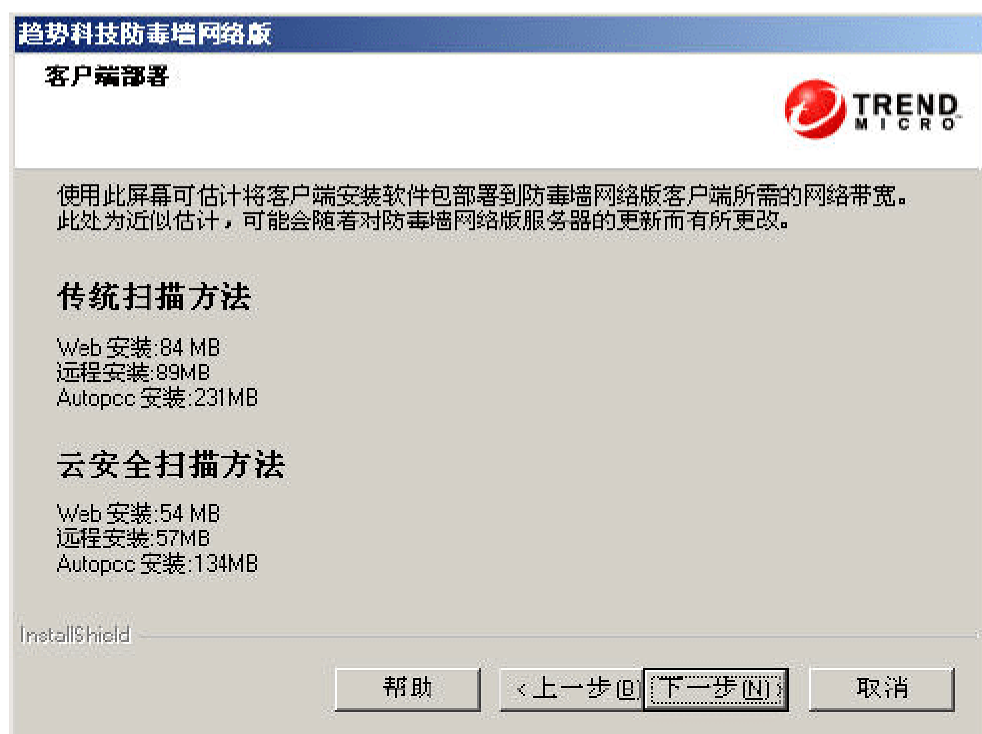


图 19-68　【客户端部署】对话框

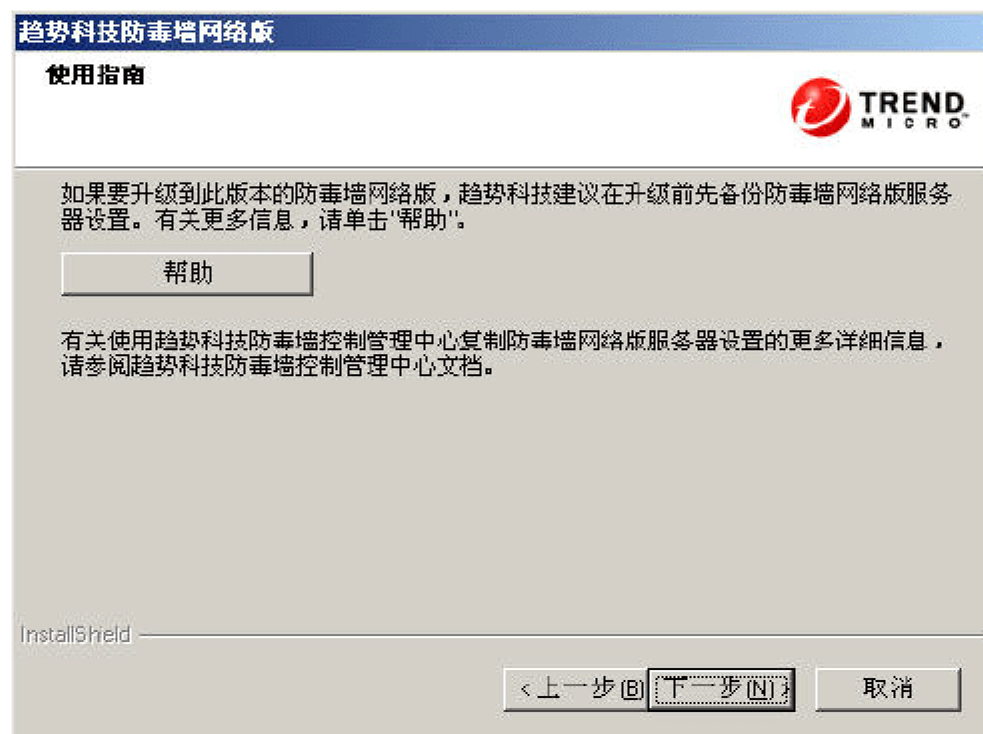


图 19-69　【使用指南】对话框

05 弹出【安装目标】对话框，选中【在此计算机上】单选按钮，如果需要将程序安装到远程主机，可以选择另一项，单击【下一步】按钮，如图 19-70 所示。

06 弹出【计算机预扫描】对话框，选中【扫描目标计算机】单选按钮，对本机进行安全风险扫描，单击【下一步】按钮，如图 19-71 所示。

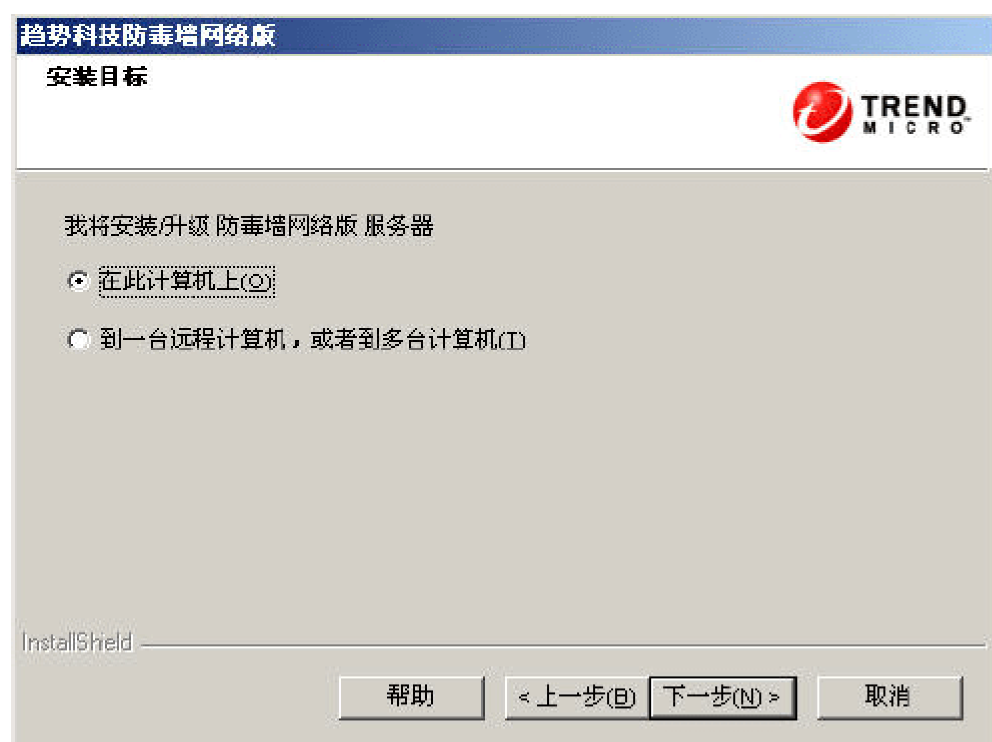


图 19-70　【安装目标】对话框

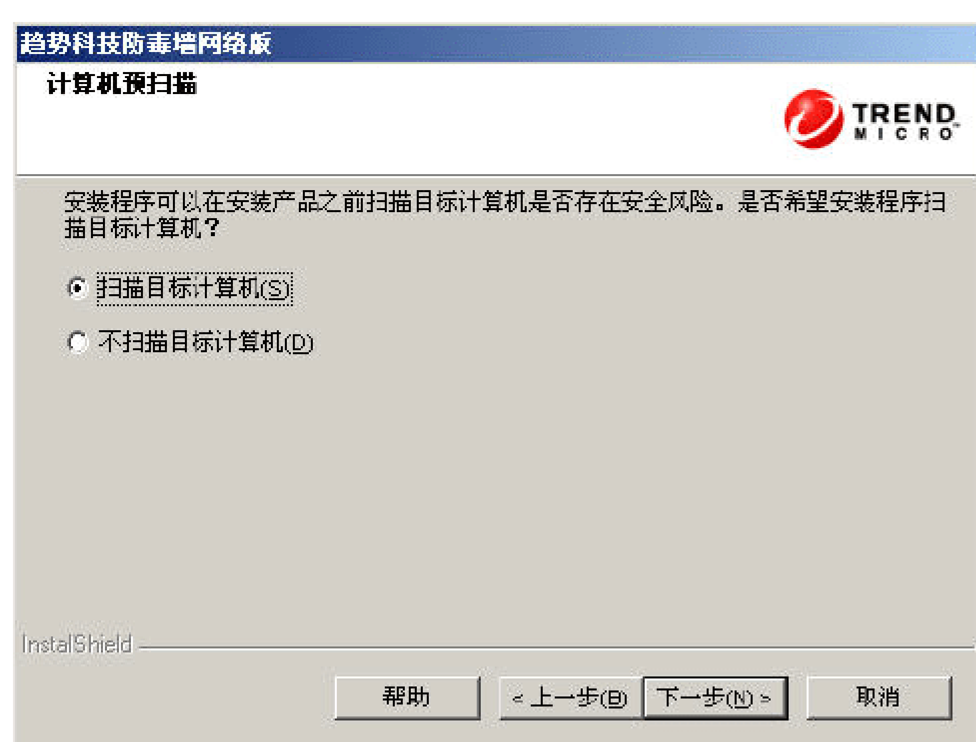


图 19-71　【计算机预扫描】对话框

07 程序自动对目标操作系统进行扫描，并显示扫描进度，如图 19-72 所示。

08 扫描结束，弹出【安装路径】对话框，单击【浏览】按钮可以设定反病毒程序的安装路径，本实例采用默认配置，单击【下一步】按钮，如图 19-73 所示。

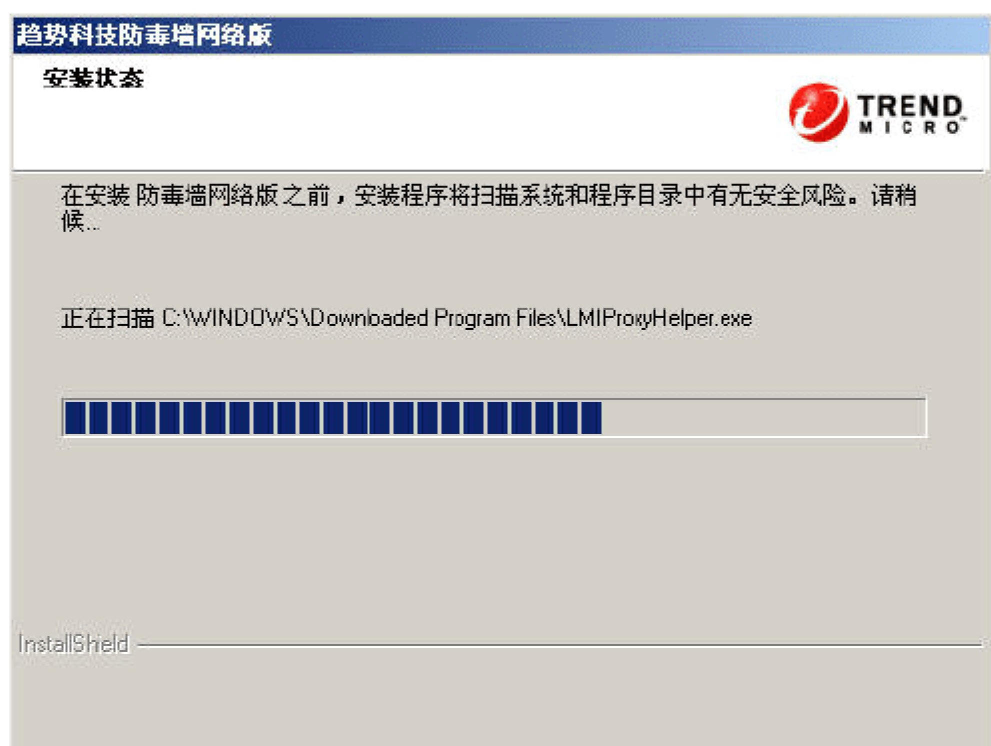


图 19-72 【安装状态】对话框

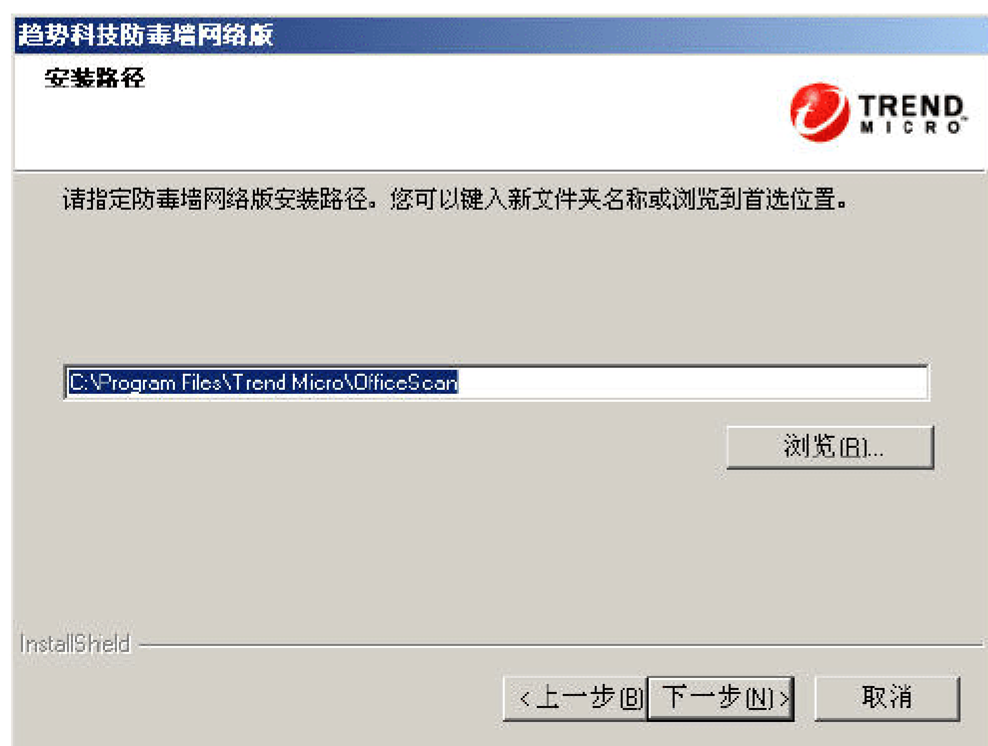


图 19-73 【安装路径】对话框

09 弹出【代理服务器】对话框，设定趋势科技企业反病毒程序访问 Internet 的代理服务器地址，本实例不作配置，单击【下一步】按钮，如图 19-74 所示。

10 弹出【Web 服务器】对话框，设置防毒墙服务器要使用的 Web 服务器，如果本机安装了 IIS 组件，可以选中【IIS 服务器】单选按钮，访问端口为 8080，如果本机没有安装 IIS 组件，只能选中【Apache Web 服务器 2.0】单选按钮，使用 Apache 服务器安全性高于 IIS 服务器，本实例使用 IIS 服务器，单击【下一步】按钮，如图 19-75 所示。

11 弹出【计算机标识】对话框，可以设定防毒墙客户端识别服务器使用 IP 地址及域名，本实例默认选中【域名】单选按钮，文本框中显示为主机名，单击【下一步】按钮，如图 19-76 所示。



图 19-74 【代理服务器】对话框

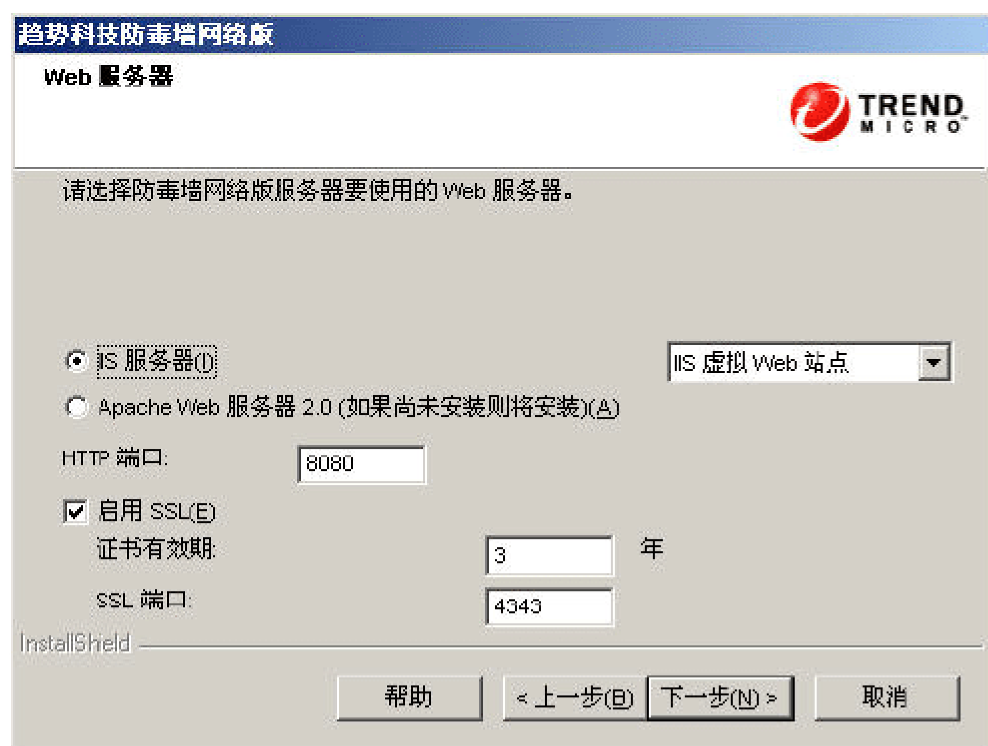


图 19-75 【Web 服务器】对话框

12 弹出【产品激活】对话框，单击【下一步】按钮，如图 19-77 所示。

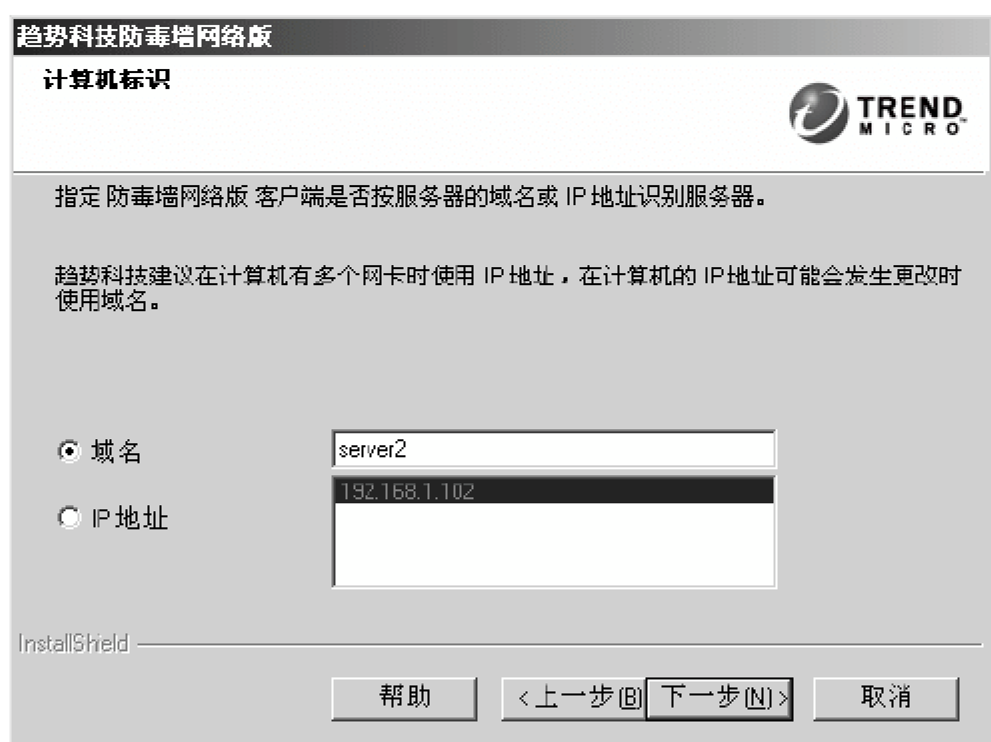


图 19-76　【计算机标识】对话框

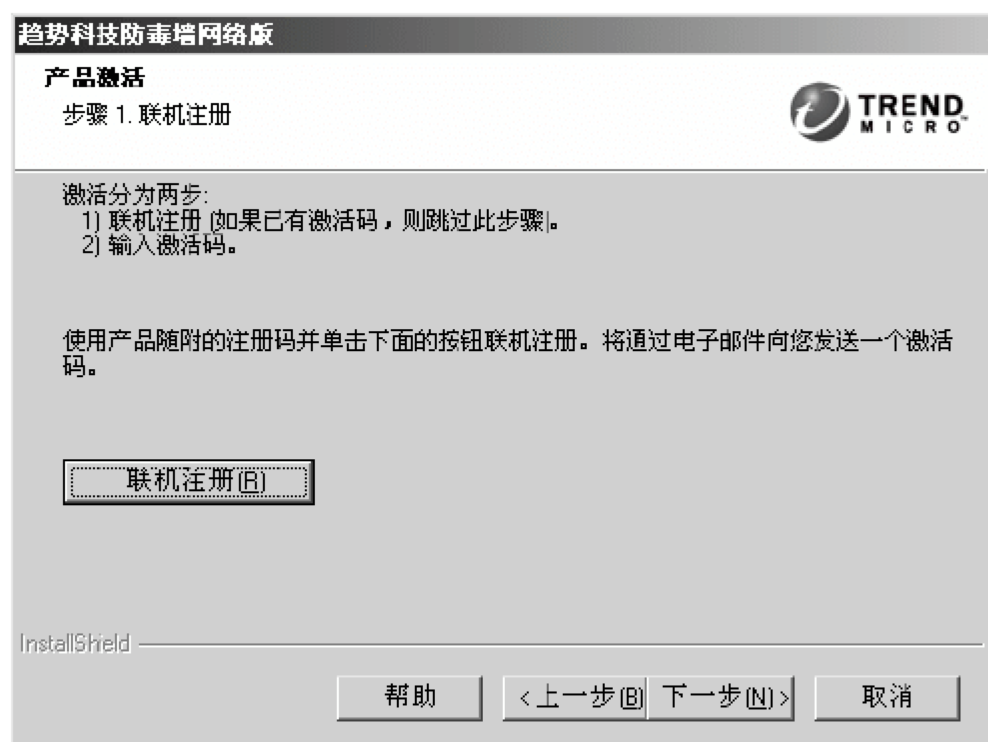


图 19-77　联机注册

13 在【防病毒】、【损害清除服务】和【Web 信誉和防间谍软件】三个文本框中，分别输入已经获得的激活码，单击【下一步】按钮，如图 19-78 所示。

14 弹出【安装集成型云安全智能防护服务器】对话框，选择默认配置，单击【下一步】按钮，如图 19-79 所示。

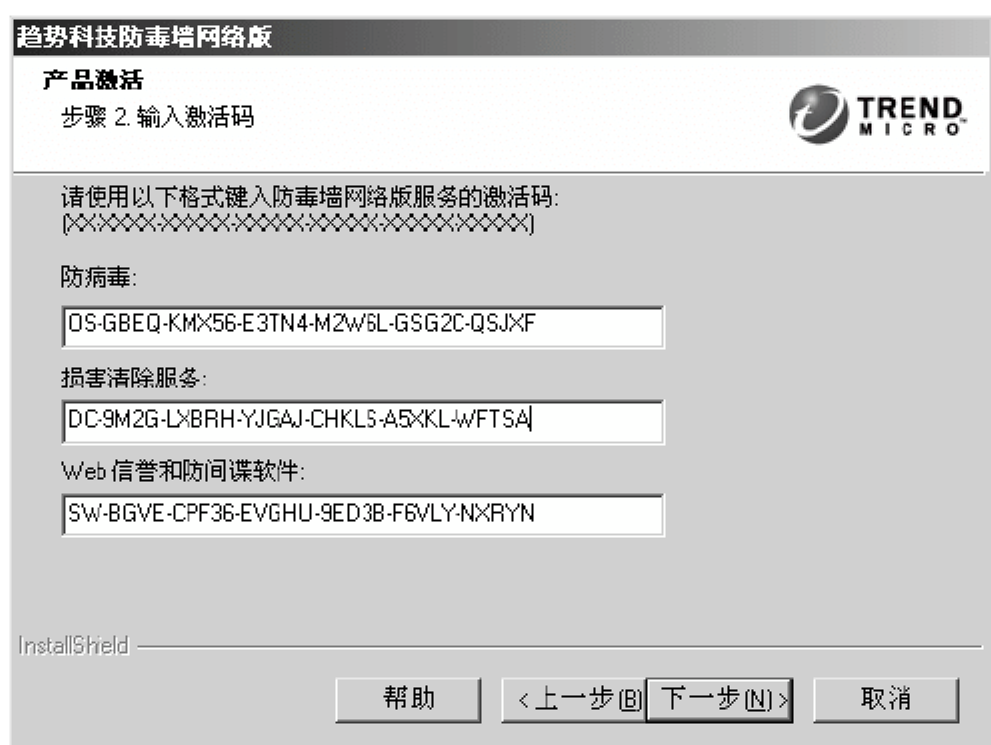


图 19-78　输入激活码

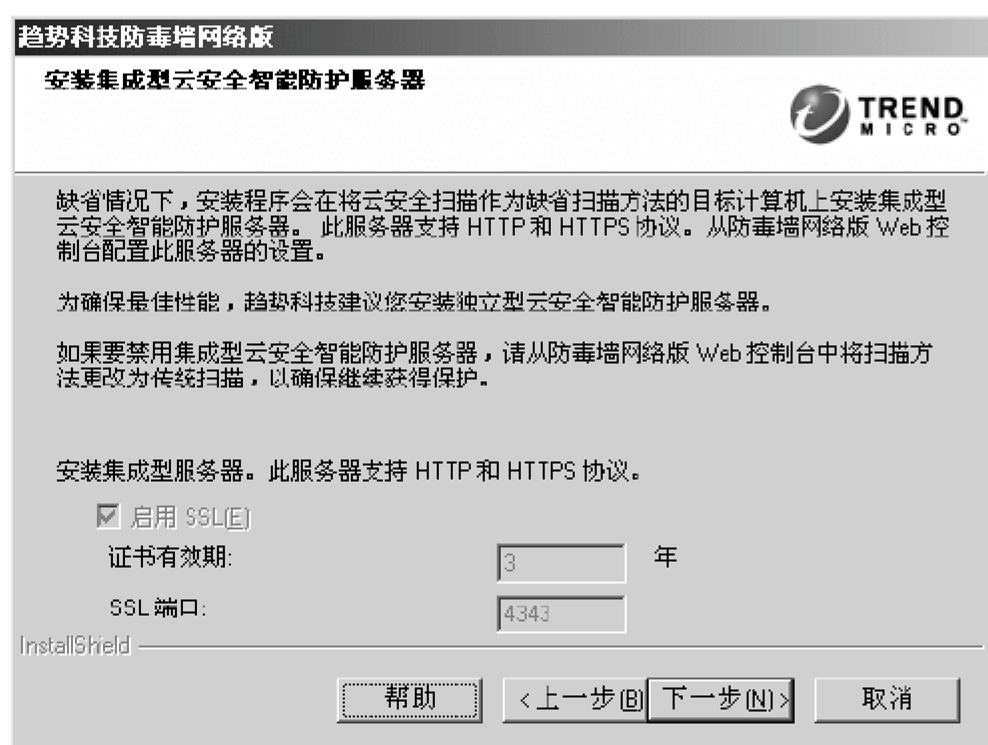


图 19-79　安装集成型云安全智能防护服务器

15 弹出【启用 Web 信誉服务】对话框，采用默认配置，单击【下一步】按钮，如图 19-80 所示。

16 弹出【安装其他防毒墙网络版程序】对话框，选择安装【防毒墙网络版客户端】程序，以确保防毒墙服务器使用客户端程序实施病毒防护（客户端程序可以实现病毒扫描、查杀），单击【下一步】按钮，如图 19-81 所示。

17 弹出【云安全智能防护网络】对话框，选中【启用趋势科技智能反馈】复选框，单击【下一步】按钮，如图 19-82 所示。

18 弹出【管理员账户密码】对话框，默认 Web 控制台访问账户为 root，根据要求在指定文本框输入密码信息，建议【Web 控制台密码】和【客户端退出与卸载密码】的信息不要相同，单击【下一步】按钮，如图 19-83 所示。

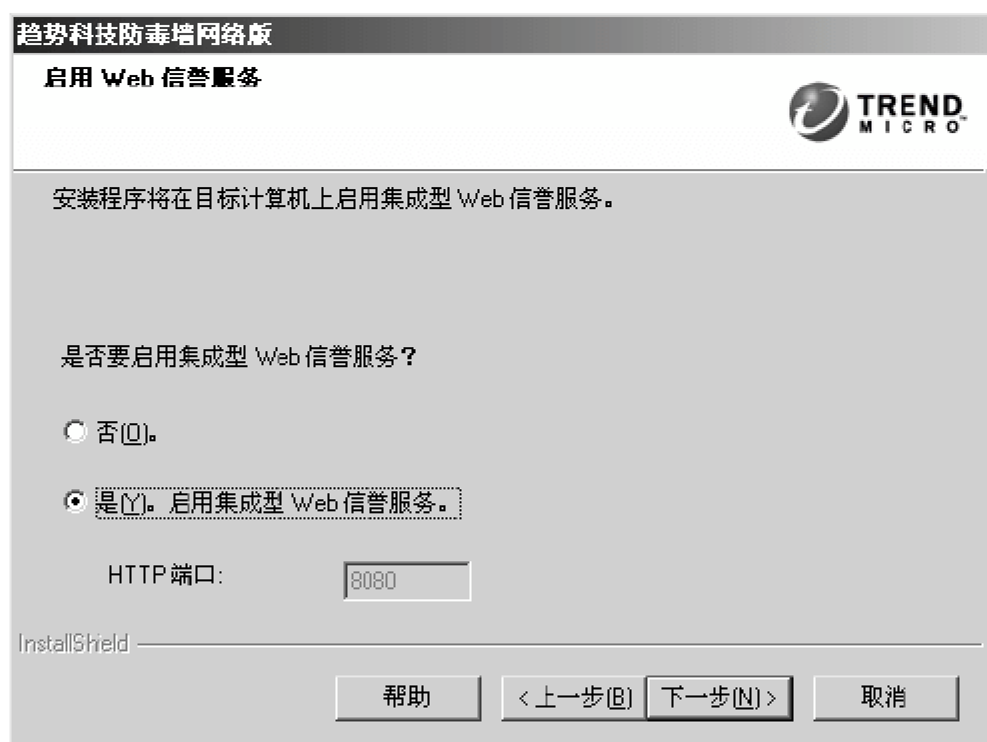


图 19-80 【启用 Web 信誉服务】对话框

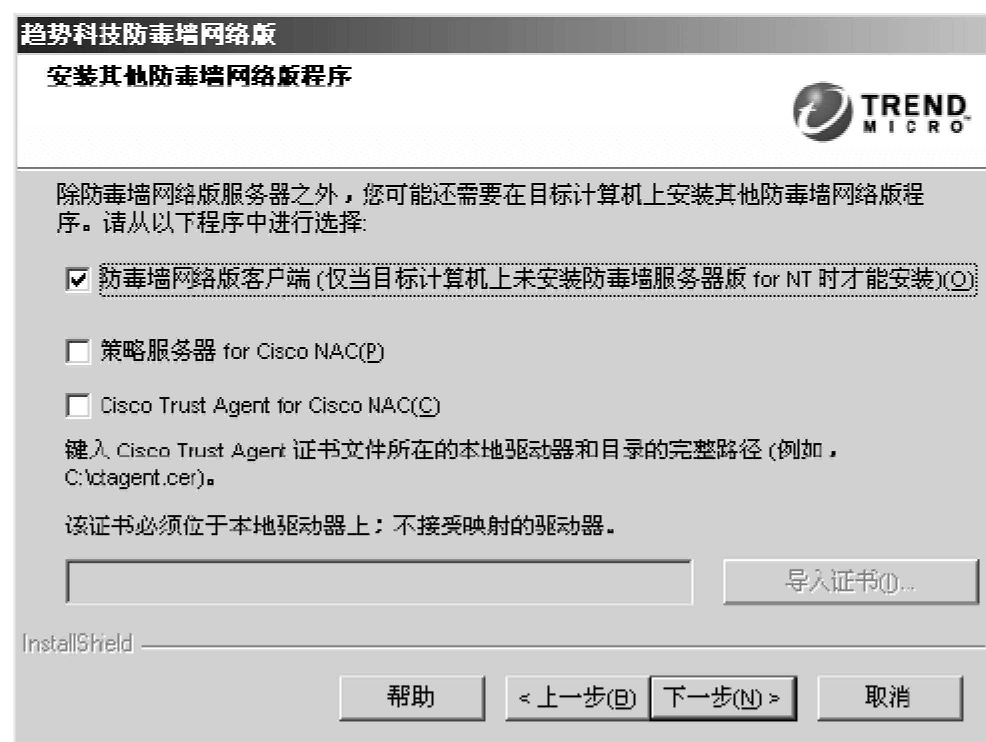


图 19-81 【安装其他防毒墙网络版程序】对话框

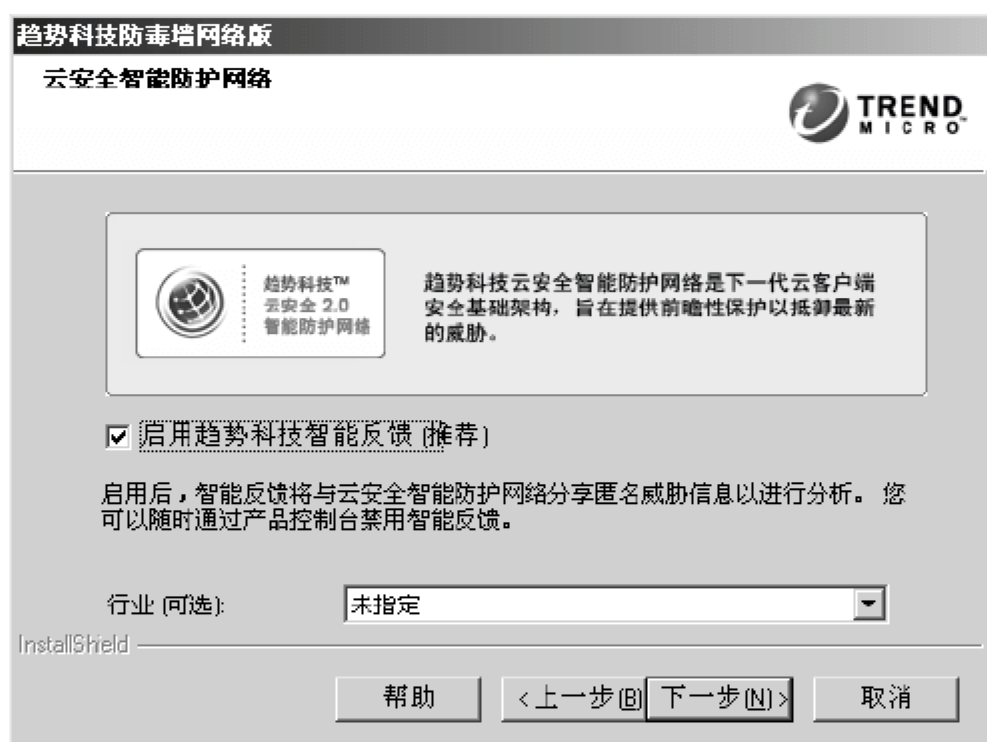


图 19-82 【云安全智能防护网络】对话框

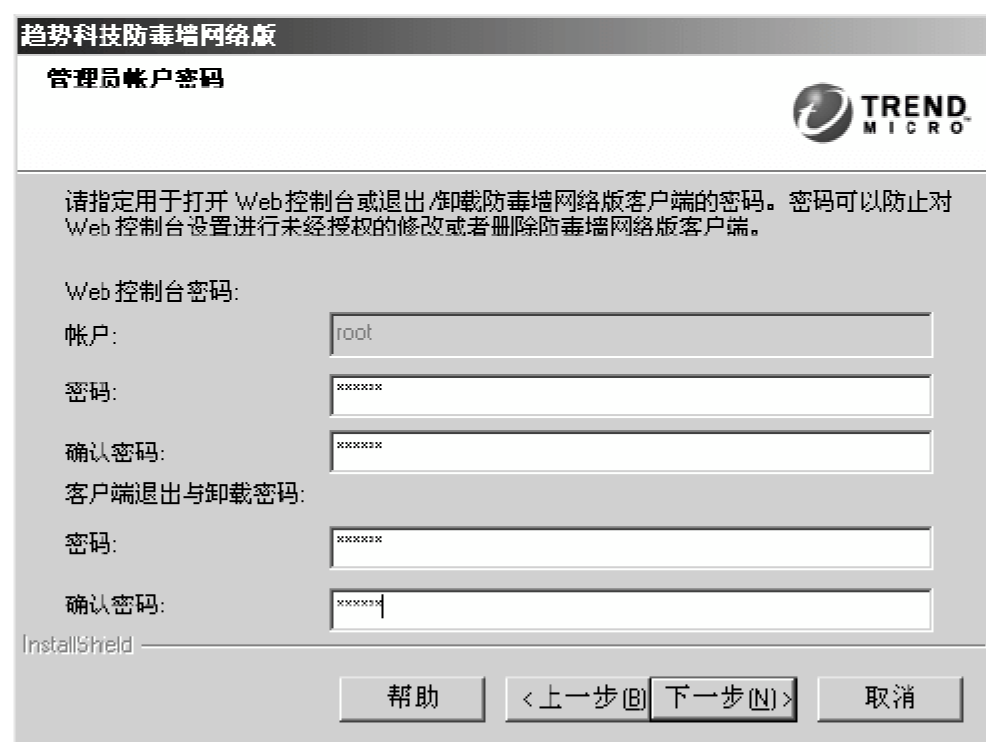


图 19-83 【管理员账户密码】对话框

19 弹出【防毒墙网络版客户端安装】对话框，设置防毒墙客户端程序的默认安装路径、访问端口及安全级别信息，本实例采用默认配置，单击【下一步】按钮，如图 19-84 所示。

20 弹出【防病毒功能】对话框，选中【启用防火墙】复选框，以确保服务器的安全，单击【下一步】按钮，如图 19-85 所示。

21 弹出【防间谍软件功能】对话框，选中【是，我想要启用评估模式】单选按钮，以防护间谍软件和灰色软件的威胁，单击【下一步】按钮，如图 19-86 所示。

22 弹出【防毒墙网络版程序快捷方式】对话框，设定在【开始】菜单中显示的程序名，采用默认配置，单击【下一步】按钮，如图 19-87 所示。



图 19-84 【防毒墙网络版客户端安装】对话框

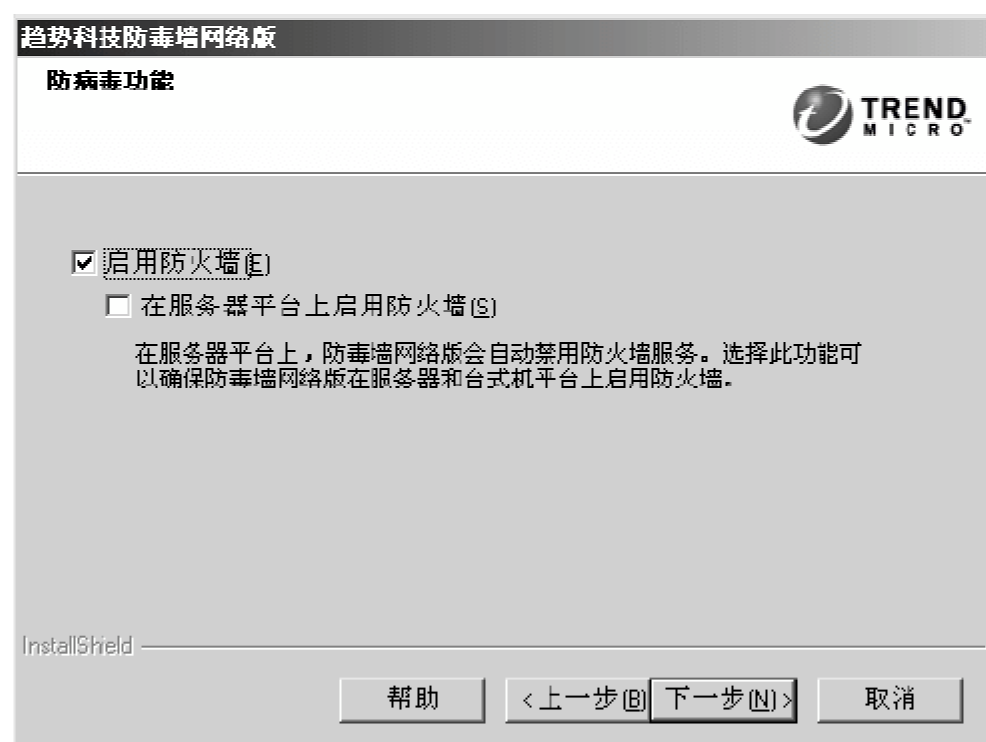


图 19-85 【防病毒功能】对话框

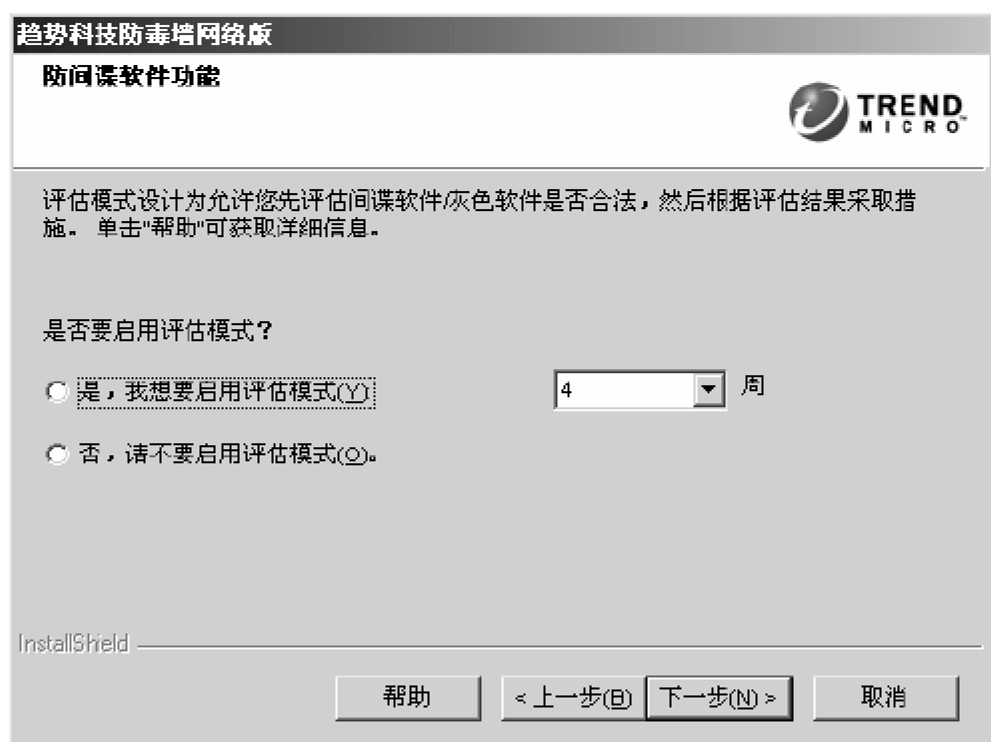


图 19-86 【防间谍软件功能】对话框

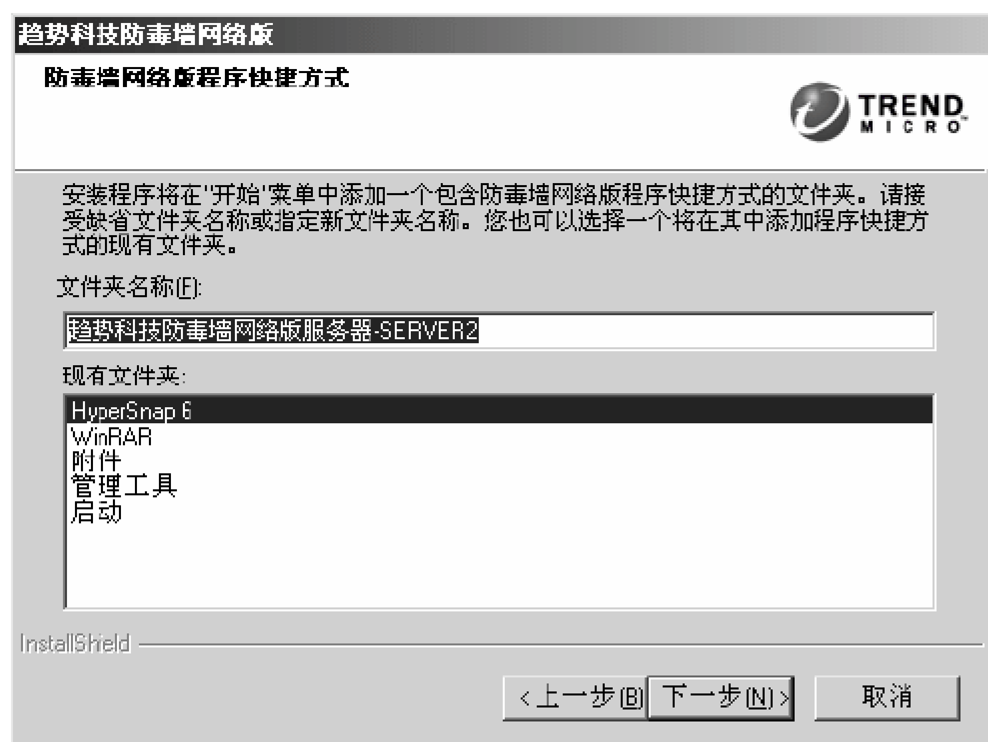


图 19-87 【防毒墙网络版程序快捷方式】对话框

23 弹出【安装信息】对话框，系统给出之前的配置摘要信息，单击【安装】按钮，如图 19-88 所示。

24 弹出【安装状态】对话框，系统依照配置自动安装程序，并显示安装进度，如图 19-89 所示。

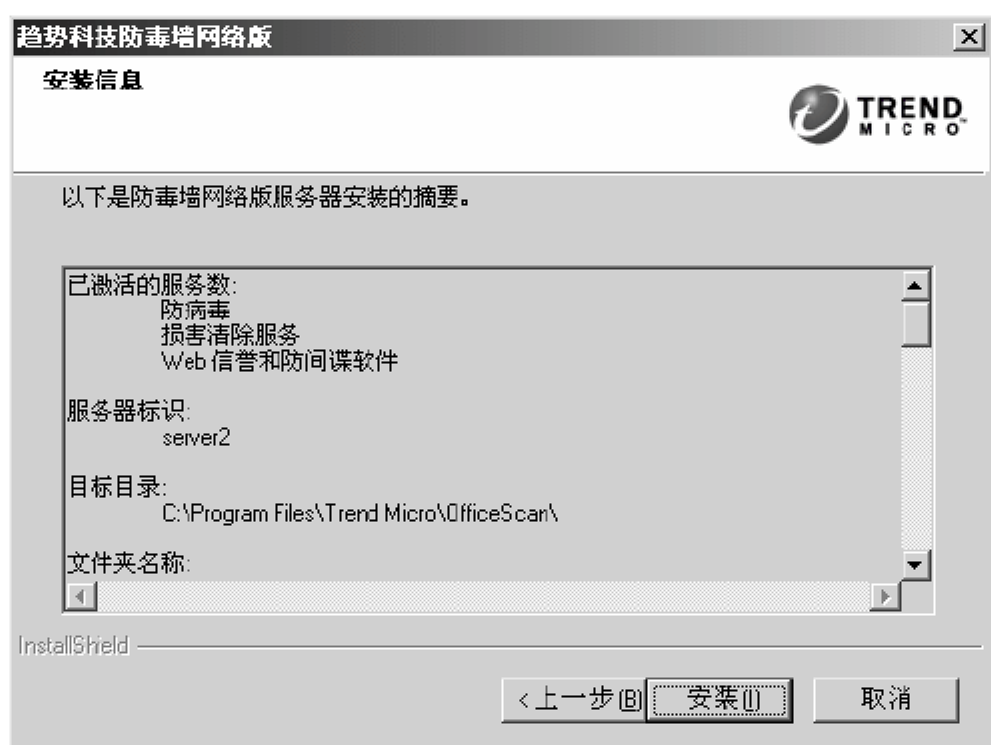


图 19-88 【安装信息】对话框



图 19-89 【安装状态】对话框

25 弹出【安装完毕】对话框，可以根据需要选中【查看自述文件】和【打开 Web 控制台】复选框，单击【完成】按钮，完成趋势科技防毒墙的安装，如图 19-90 所示。

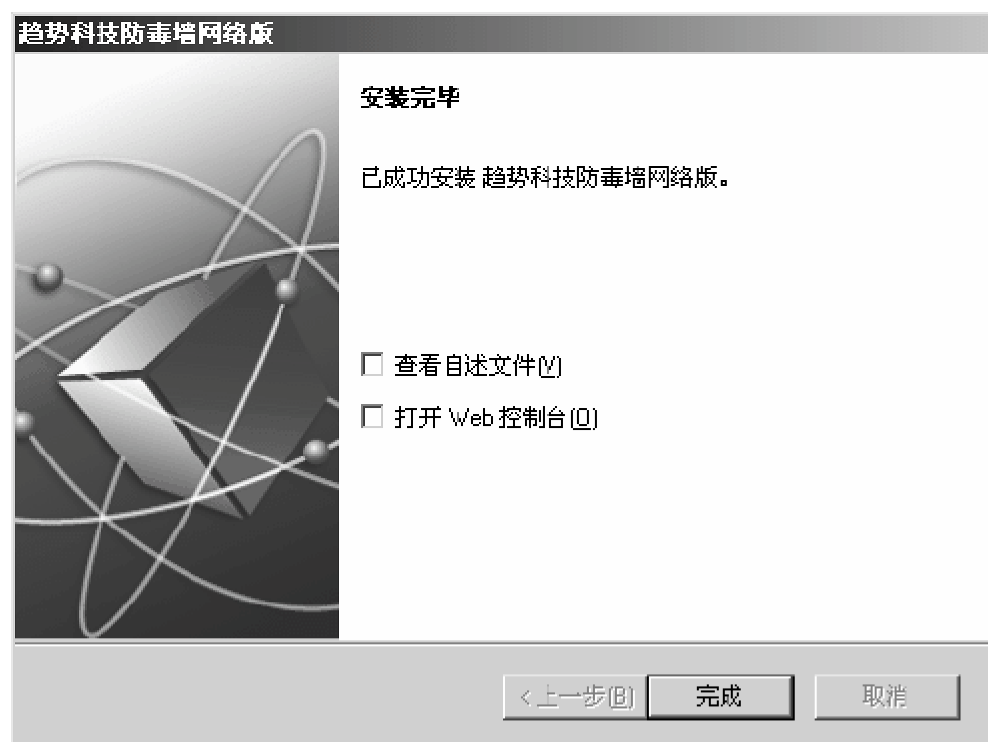


图 19-90 【安装完毕】对话框

19.3.2　设置趋势科技软件防护内网安全

在使用趋势科技软件进行全网杀毒之前，需要设置趋势科技软件以防护内网安全。

1. 登录趋势科技 Web 控制台

01 选择【开始】➢【程序】➢【趋势科技防毒墙网络版服务器】➢【防毒墙网络版 Web 控制台（HTML）】命令，如图 19-91 所示。

02 弹出【安全警报】对话框，单击【是】按钮，如图 19-92 所示。



图 19-91　防毒墙网络版 Web 控制台（HTML）

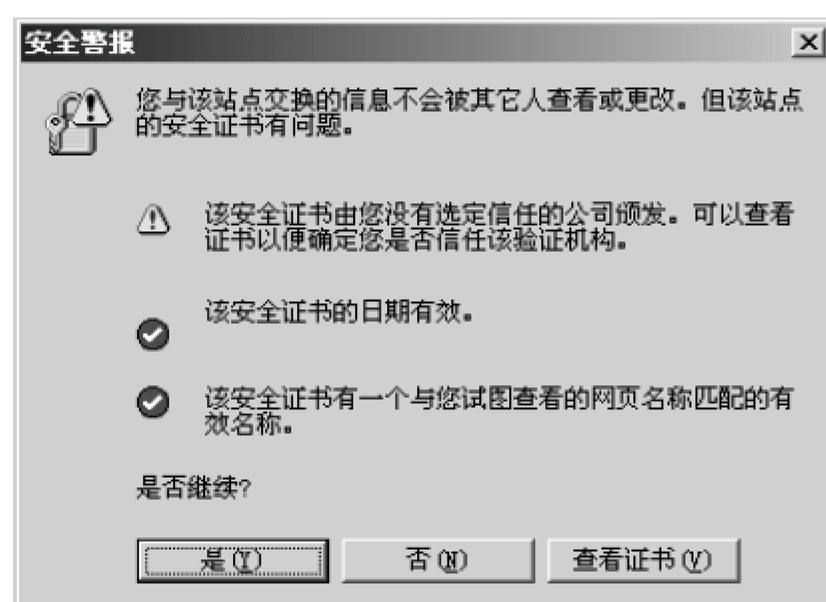


图 19-92　【安全警报】对话框

03 进入【WEB 控制台登录】页面，在【用户名】和【密码】文本框中分别输入有效信息，本实例采用默认账户 root 和安装时设定的密码 123123，单击【登录】按钮，如图 19-93 所示。

04 进入趋势科技防毒墙网络版程序主页面，同时弹出【Internet Explorer-安全警报】对话框，提示安装程序必要组件，单击【安装】按钮，如图 19-94 所示。



图 19-93　【WEB 控制台登录】页面



图 19-94　【安全警告】提示框

05 组件安装成功，显示程序主界面，默认显示【摘要】信息，包括客户端联机状态、病毒爆发状态、联网计算机更新状态等信息，如图 19-95 所示。



图 19-95　趋势科技防病毒程序主界面

2．添加防毒墙客户端

想要对全网主机实施反病毒，必须将这些主机加入到反病毒系统中，因此，需要在所有主机内安装防毒墙客户端程序。安装方法有两种，分别是基于浏览器安装和远程安装。

1）基于浏览器安装

基于浏览器安装防毒墙客户端程序的具体的操作步骤如下。

01 在图 19-95 所示主界面的左侧选项列表中选择【联网计算机】➢【客户端安装】➢【基于浏览器】选项，在右侧界面的【电子邮件主题】文本框中设置客户端接收邮件的主题，本实例采用默认配置，单击【创建电子邮件】按钮，如图 19-96 所示。

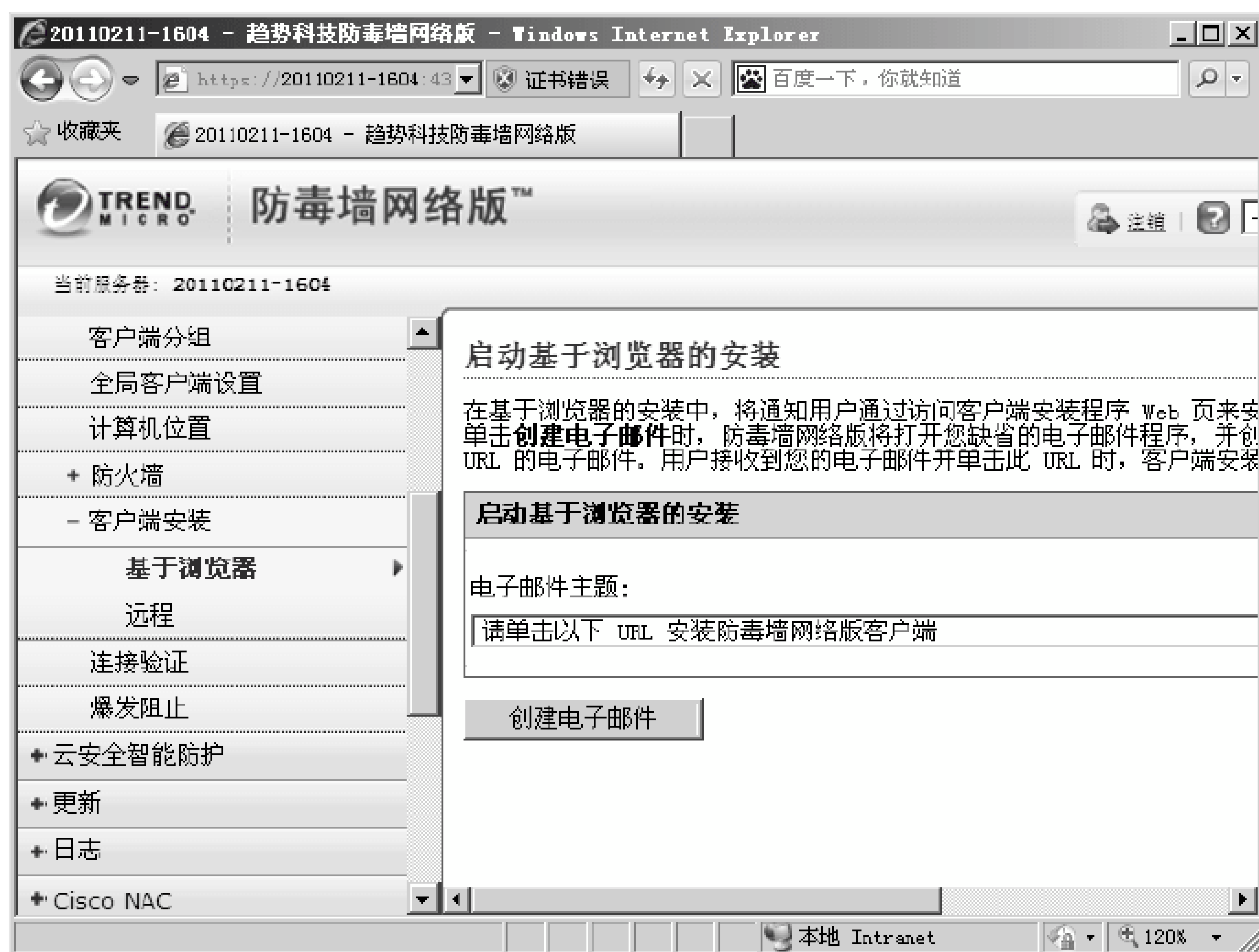


图 19-96　基于浏览器安装防毒墙客户端

02 在弹出的窗口中可以设置邮件信息，在【收件人】文本框中输入收件人的邮箱地址，本

实例使用“user@163.com”进行演示，其他采用默认配置，单击【发送】按钮，如图 19-97 所示。

03 本地没有发件人信息，所以首先要添加发件人，在弹出的【您的姓名】对话框中设置发件人显示名为“user2”，单击【下一步】按钮，如图 19-98 所示。

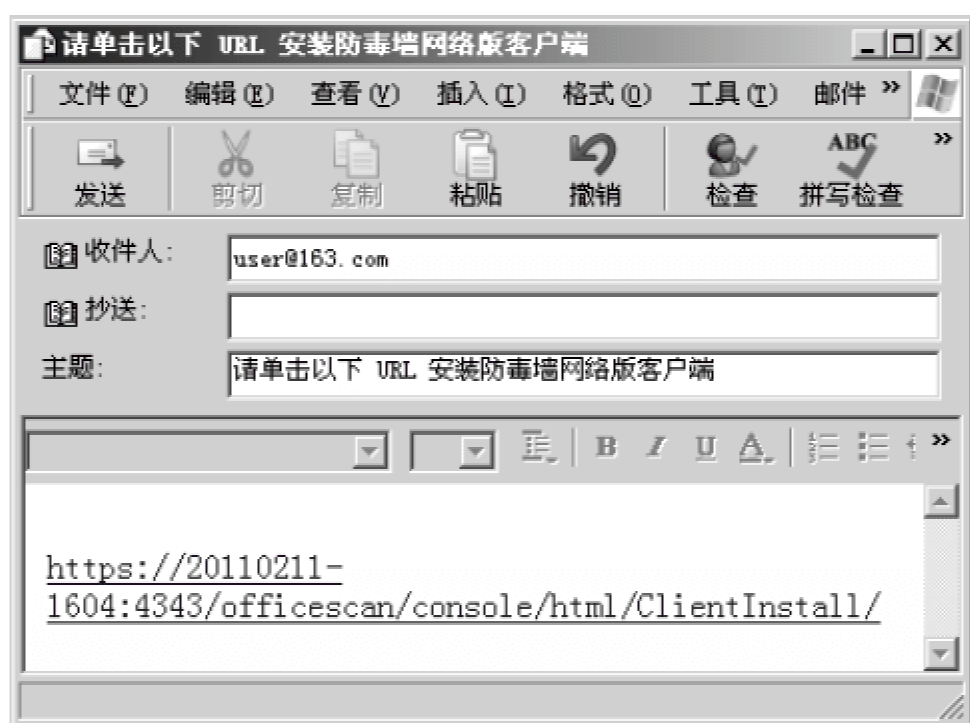


图 19-97 编辑邮件信息



图 19-98 创建邮箱发件人

04 弹出【Internet 电子邮件地址】对话框，在【电子邮件地址】文本框中输入发件人邮箱地址，本实例使用“user2@163.com”，单击【下一步】按钮，如图 19-99 所示。

05 弹出【电子邮件服务器名】对话框，在【接收邮件服务器】和【发送邮件服务器】文本框中输入正确地址信息，由于本案例使用的是 163 邮箱，所以服务器使用如图 19-100 所示配置，单击【下一步】按钮。



图 19-99 【Internet 电子邮件地址】对话框

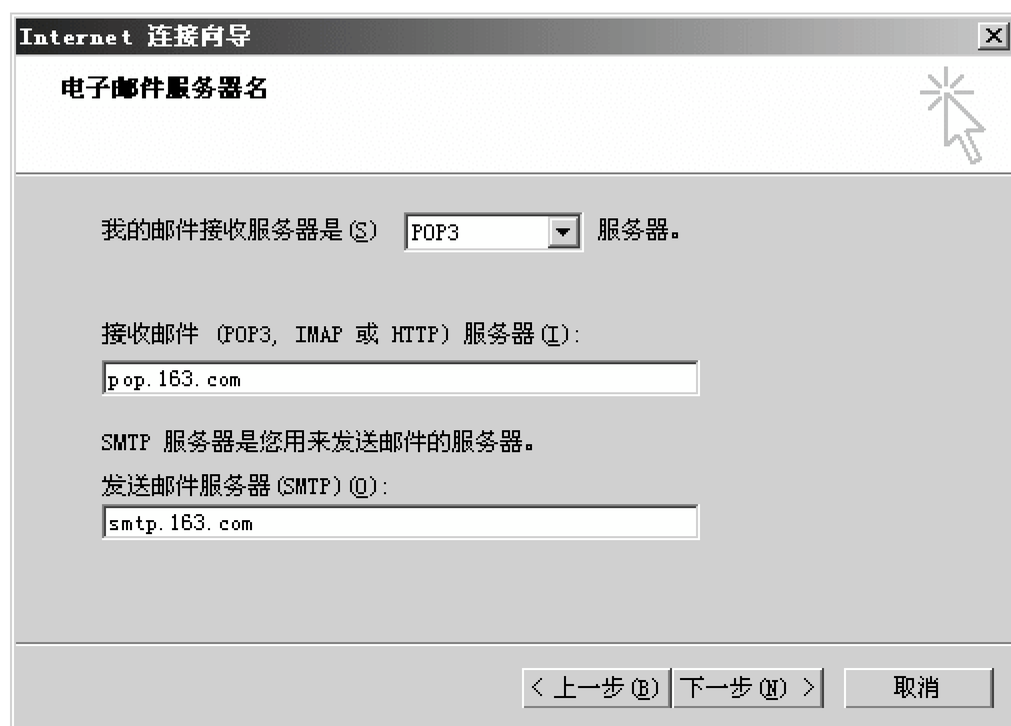


图 19-100 【电子邮件服务器名】对话框

06 弹出【Internet 邮件登录】对话框，在【账户名】文本框中输入“user2”，在【密码】文本框中输入指定邮箱的有效密码，单击【下一步】按钮，如图 19-101 所示。

07 弹出【祝贺您】对话框，邮件账户设置成功，单击【完成】按钮，向客户端发送邮件，如图 19-102 所示。

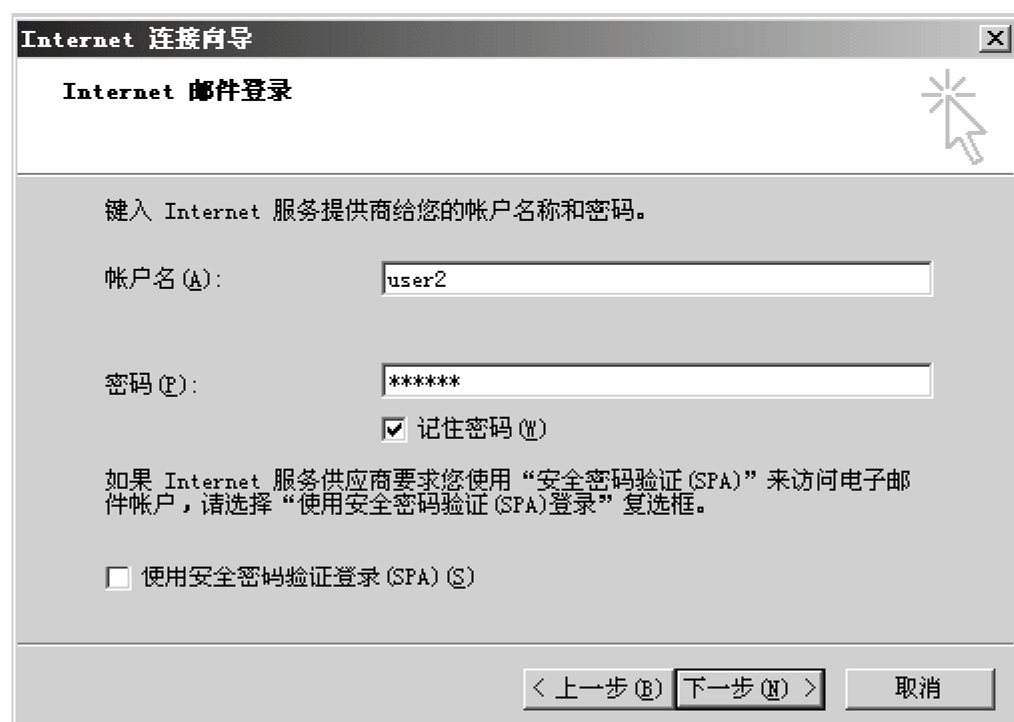


图 19-101　【Internet 邮件登录】对话框

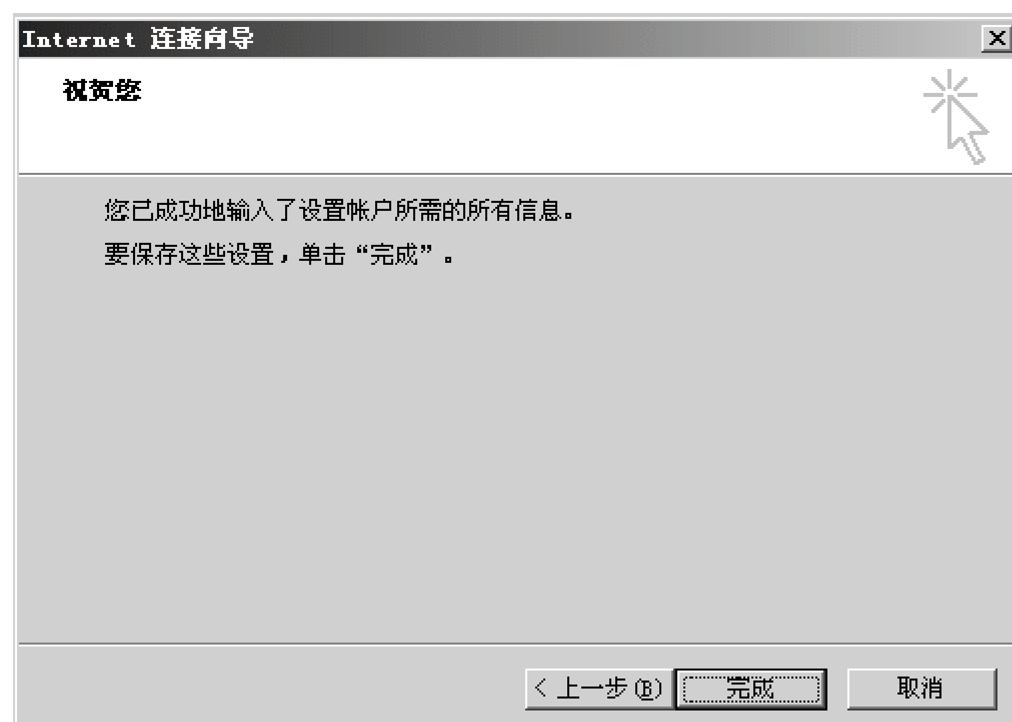


图 19-102　【祝贺您】对话框



提　示

本实例中采用的邮箱地址及密码必须是当前网络可用的有效地址。

2）远程安装

使用这种方法必须要有访问客户机的权限和有效的计算机账户与密码。远程安装的具体操作步骤如下。

01 在图 19-95 所示主界面的左侧选项列表中选择【联网计算机】➢【客户端安装】➢【远程】选项，右侧显示【远程安装】窗格。在【计算机名称】文本框中可以输入需要安装防毒墙客户端的客户机名称或 IP 地址，本实例以“192.168.1.103”主机为例进行讲解，单击【搜索】按钮，如图 19-103 所示。

02 在弹出的对话框的【用户名】和【密码】文本框中，分别输入指定客户机的认证信息，单击【登录】按钮，如图 19-104 所示。

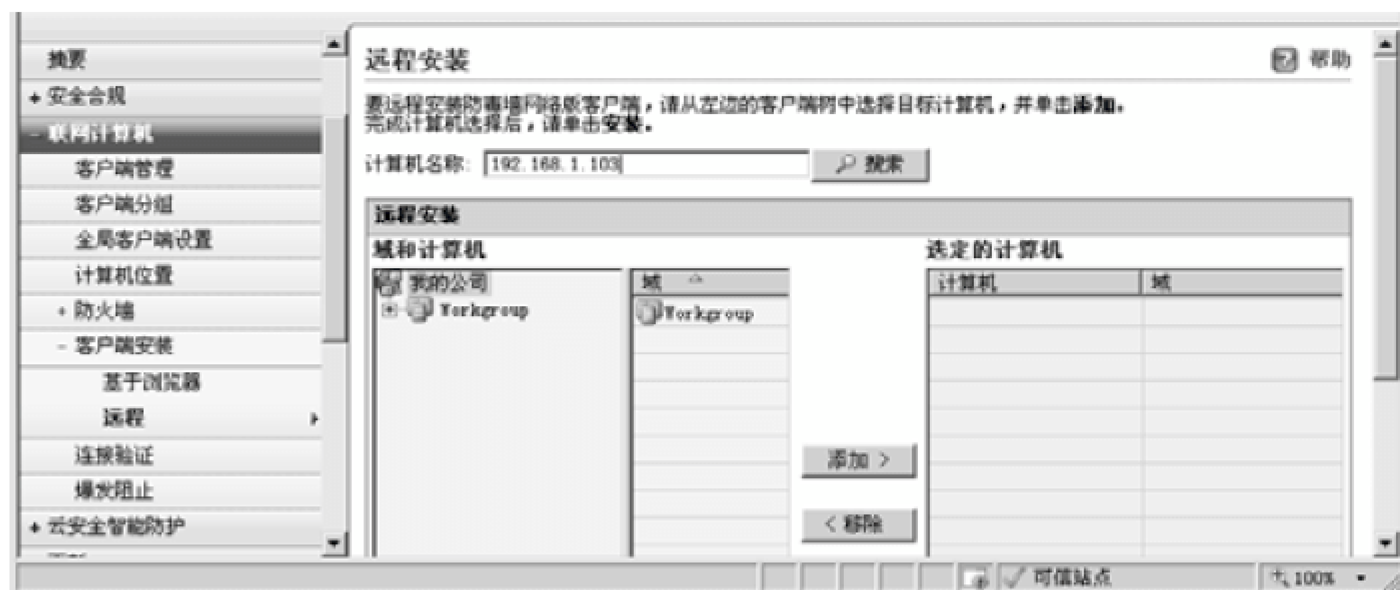


图 19-103　远程安装防毒墙客户端



图 19-104　登录提示框

03 登录成功，在右侧的【选定的计算机】列表中显示了已连接成功的计算机，单击窗格左下角的【安装】按钮，如图 19-105 所示。

04 弹出【趋势科技防毒墙网络版管理控制台】对话框，提醒是否在指定的“192.168.1.103”计算机上安装客户端程序，单击【是】按钮，如图 19-106 所示。



图 19-105　向选定的计算机安装客户端

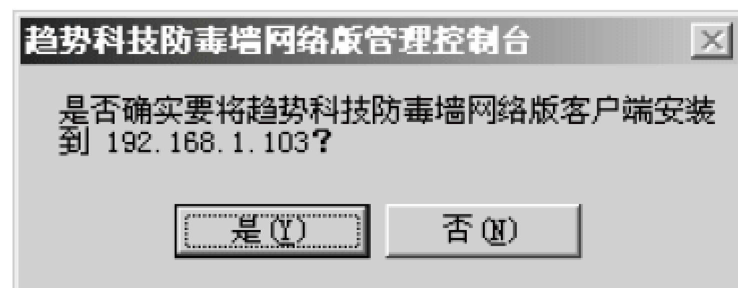


图 19-106　安装提示框

05 自动安装客户端程序，安装成功后弹出如图 19-106 所示的对话框，单击【确定】按钮。

06 返回程序控制台页面，右侧【选定的计算机】列表中“192.168.1.103”计算机图标被选中，如图 19-108 所示。

以上方法每次只能连接一台客户机，要想同时连接多台客户机，可以使用如下操作方法完成。

在【域和计算机】窗格中显示了系统自动扫描到的工作组网络中的计算机信息，选中需要添加的计算机，单击【添加】按钮，可将其加入到右侧【选定的计算机】窗格中，被选定的计算机可以通过单击【安装】按钮完成客户端安装。



图 19-107　安装结果提示框



图 19-108　防病毒客户端安装成功

3．管理客户端

防毒墙客户端安装完成后，需要对这些客户端进行管理。

管理客户端的具体操作步骤如下。

01 在左侧列表中选择【联网计算机】➢【客户端管理】选项，展开右侧【客户端管理】页面，该页面可以显示出客户端计算机列表，也可以对指定的计算机进行管理操作，如图 19-109 所示。



图 19-109　查看客户端管理

02 选中一台客户机，单击【状态】按钮，可设置客户端的状态，如已连接的客户端可被设置为断开，如图 19-110 所示。



图 19-110　设置客户端状态

03 选中一台或多台客户机，单击【任务】按钮，打开其下拉列表，可以对选中的客户机执行三种操作，分别是【立即扫描】、【客户端卸载】和【间谍软件/灰色软件恢复】，如图 19-111 所示。

04 单击【设置】按钮，打开其下拉列表，可对客户机实施多种设置内容，如图 19-112 所示。

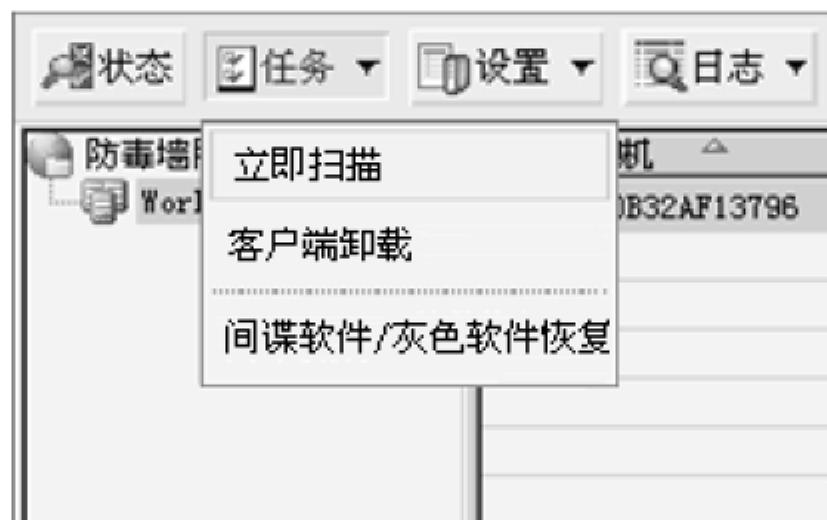


图 19-111　为客户端定制任务



图 19-112　配置客户端扫描设置

【设置】下拉列表中各选项的含义如下。

- 扫描方法

如图 19-113 所示，对客户端进行扫描的方法有两种，分别是【传统扫描】和【云安全扫描】。考虑到安全时效问题，一般建议选择【云安全扫描】。因为本地存储的病毒库更新不及时，会导致无法防御新病毒的威胁；而云端存储的病毒库因有互联网提供新病毒资源，更新会快很多。但是如果网络环境的互联网连接不是很稳定，为了避免扫描失败可以选择【传统扫描】。

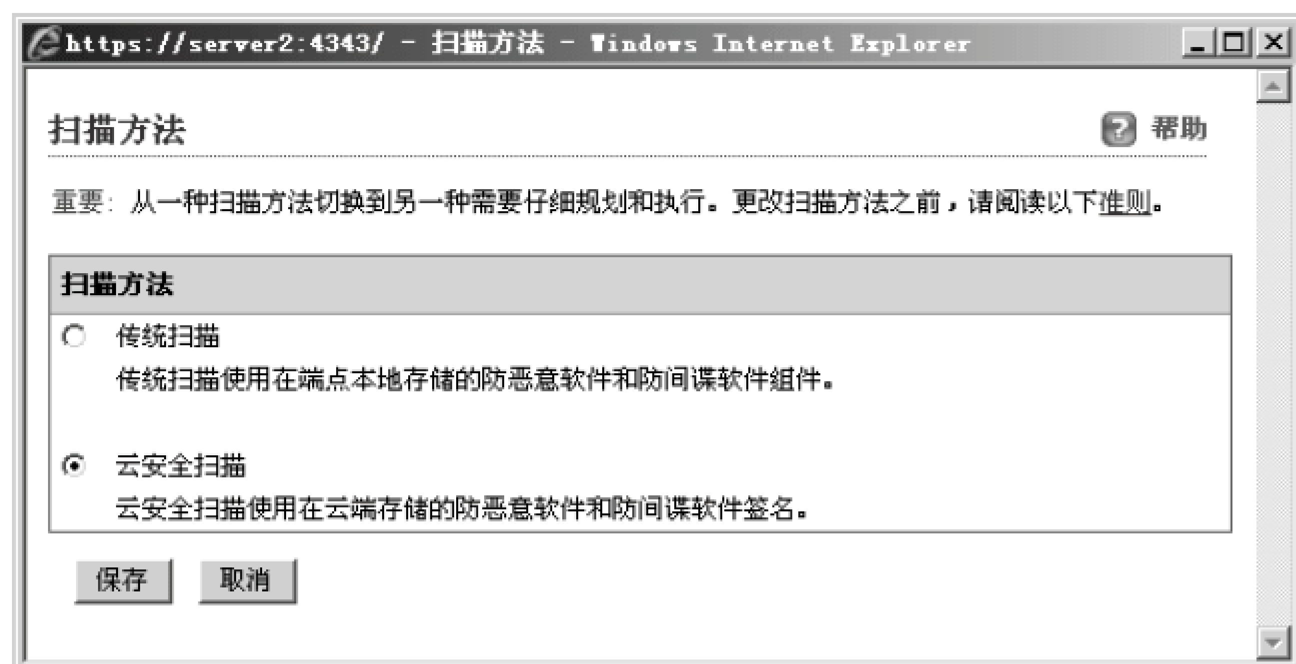


图 19-113　设置客户端扫描方法

- 手动扫描设置

当发现威胁时，管理员可以手动进行病毒扫描。【手动扫描设置】主要分为两部分，即【目标】和【处理措施】。

【目标】主要用于确定扫描对象。【要扫描的文件】选项用于指定需要扫描的文件类型，默认选中【IntelliScan】单选按钮。【扫描设置】选项用于指定特殊扫描设置，如压缩文件的扫描深度，是否扫描隐藏文件等，如图 19-114 所示。

【处理措施】用于确定如何处理扫描出的病毒、木马。可根据需求进行配置，一般选择默认值，如图 19-115 所示。



图 19-114　【目标】选项卡



图 19-115　【处理措施】选项卡

● 实时扫描设置

日常应用中，反病毒程序会实时监控网络状态，防止病毒、木马攻击。实时监控网络安全状态的扫描采用【实时扫描设置】，如图 19-116 所示。

● 预设扫描设置

为了安全，经常会设置一些定时的扫描任务，这类任务称为预设扫描任务，采用【预设扫描设置】，如图 19-117 所示。



图 19-116　【实时扫描设置】页面



图 19-117　【预设扫描设置】页面

- 立即扫描设置

配置【立即扫描设置】项后，系统会直接应用该项的配置进行扫描，如图 19-118 所示。

05 单击【日志】按钮，打开其下拉列表，可以通过多项设置进行日志管理，选择【病毒/恶意软件日志】选项，如图 19-119 所示。



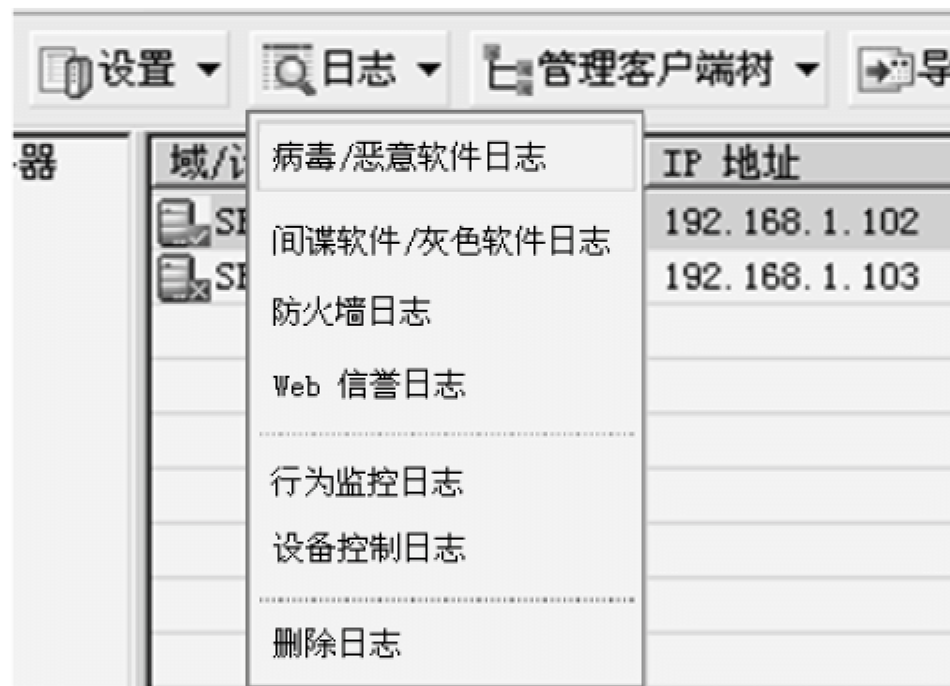


图 19-118 【立即扫描设置】页面

图 19-119 配置程序日志设置

06 弹出【病毒/恶意软件日志条件】页面，可以设定记录日志的条件，默认记录七天内的所有扫描类型的日志，并按照时间进行排序保存，单击【显示日志】按钮，可以查看已存日志，如图 19-120 所示。

07 单击【管理客户端树】按钮，打开其下拉列表，有多项配置可以用于管理客户端树。这些项目主要用于层次化的管理客户端，如图 19-121 所示。

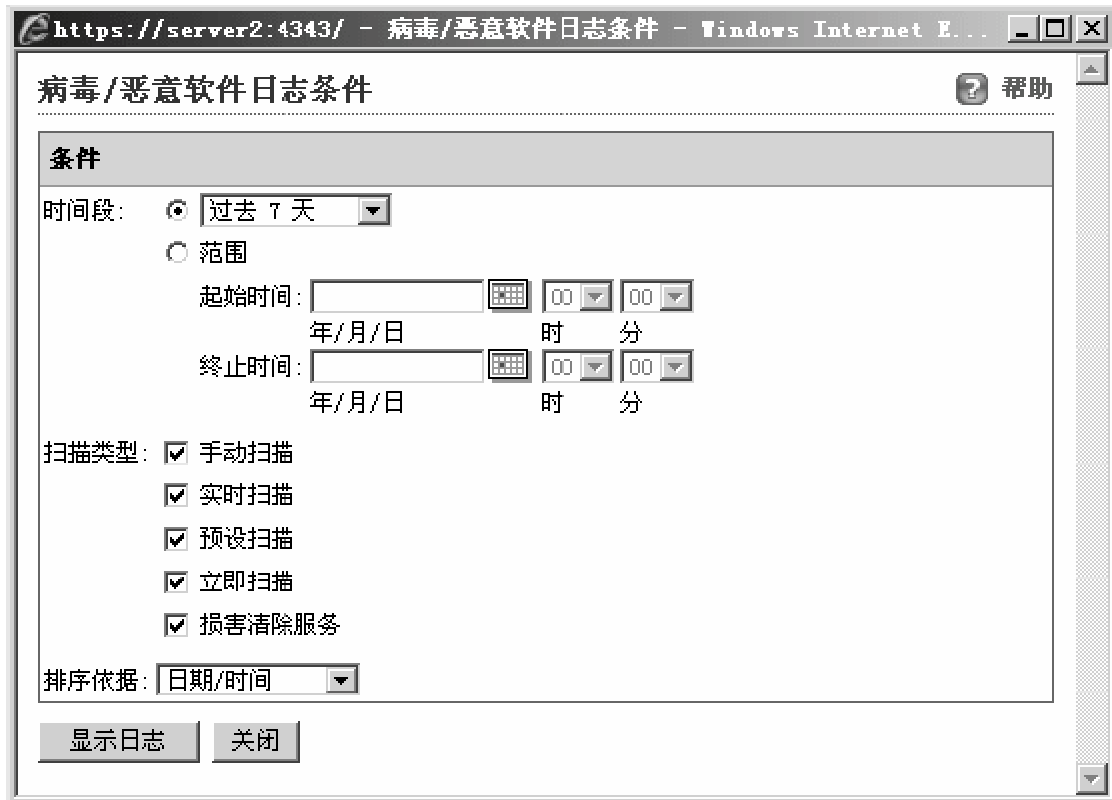




图 19-120 【病毒/恶意软件日志条件】页面

图 19-121 管理客户端树

● 添加域

在【域名】文本框中可以输入新的区域名，该区域名可以按照部门、职能、地理进行添加，输入后单击【添加】按钮，如图 19-122 所示。

如图 19-123 所示，新添加了一个区域，名称为 Server1。



图 19-122　【添加域】页面



图 19-123　新域添加成功

● 移动客户端

添加了新区域后，需要把对应的客户端加入到该域。首先选择指定的客户端，选择图 19-121 所示的【移动客户端】命令，在弹出的【移动客户端】页面选择指定的区域名，单击【移动】按钮，如图 19-124 所示。

移动成功，已将一台客户端移动到了 Server1 区域中，如图 19-125 所示。



图 19-124　【移动客户端】页面



图 19-125　客户端移动成功

4. 爆发阻止

当网络中某一主机感染病毒后，不及时处理很可能会将其病毒散播到全网络，造成巨大的损失，此时只要将该主机从当前网络中断开，单独查杀病毒即可解决问题。

通过趋势科技网络版防毒墙可以进行网络扫描，及时发现感染病毒的主机，同时可以利用其

【爆发阻止】功能将被感染主机网络暂时断开，进行病毒清理。具体的操作方法为：在左侧列表中选择【联网计算机】➢【爆发阻止】选项，右侧显示【爆发阻止】窗格，在列表中选择指定需要开启【爆发阻止】功能的计算机，单击【启动爆发阻止】按钮即可，如图 19-126 所示。



图 19-126 启动爆发阻止

19.3.3 使用趋势科技软件进行全网杀毒

在使用趋势科技进行网络杀毒时，主要有两种方式，分别是管理员统一全网杀毒和客户机自主杀毒。

1. 全网同步杀毒

当网络中感染病毒后，只是单一地对个别主机进行病毒查杀并不能彻底清除病毒，当病毒突然爆发时，依靠计划任务也不现实，这就需要管理员进行全网同步杀毒操作，具体的操作步骤如下。

01 选择程序主页面左侧列表中的【立即扫描所有域】选项，弹出【立即扫描】页面，可以实现全网病毒扫描，如图 19-127 所示。

02 在该页面中选择需要扫描的计算机，单击【启动立即扫描】按钮，开始扫描。



图 19-127 配置扫描所有域



图 19-128 【立即扫描】页面

03 扫描结束后，弹出一个信息提示框，提示用户确认收到通知的客户端只有一个，另一个可以尝试重新连接扫描，如图 19-129 所示。



还可以在程序主界面中选择【联网计算机】➢【客户机管理】选项，在右侧窗格中选择所有计算机，选择【任务】下拉列表中的【立即扫描】命令实现全网扫描。

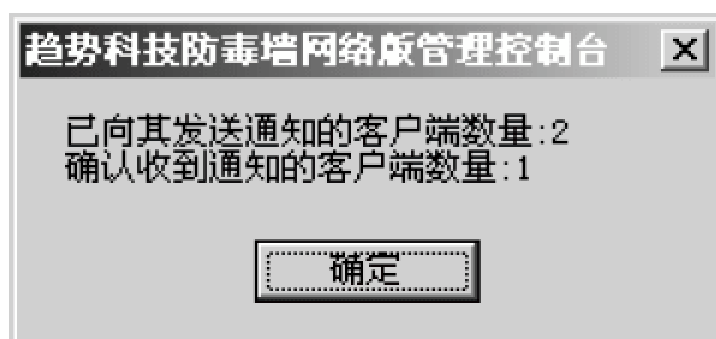


图 19-129　客户端扫描结果提示框

当客户机感染病毒后，为了及时清理，用户可以手动对自己的主机进行病毒查杀，具体的操作步骤如下。

01 运行趋势科技客户端防毒软件，弹出图 19-130 所示的窗口，在【手动扫描】选项卡中选择需要扫描的驱动器符号，单击【扫描】按钮，开始扫描选择驱动磁盘。

02 扫描完成后，在【手动扫描结果】选项卡中显示了扫描结果，如图 19-131 所示。

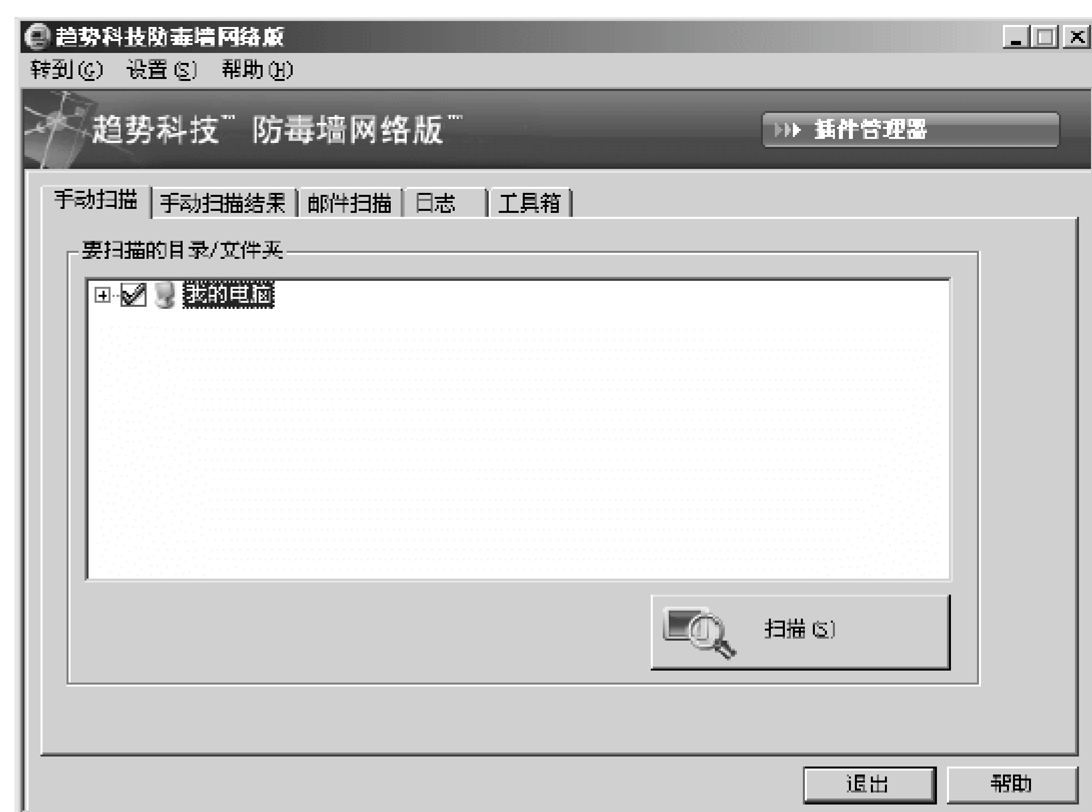


图 19-130　趋势科技防毒客户端程序界面

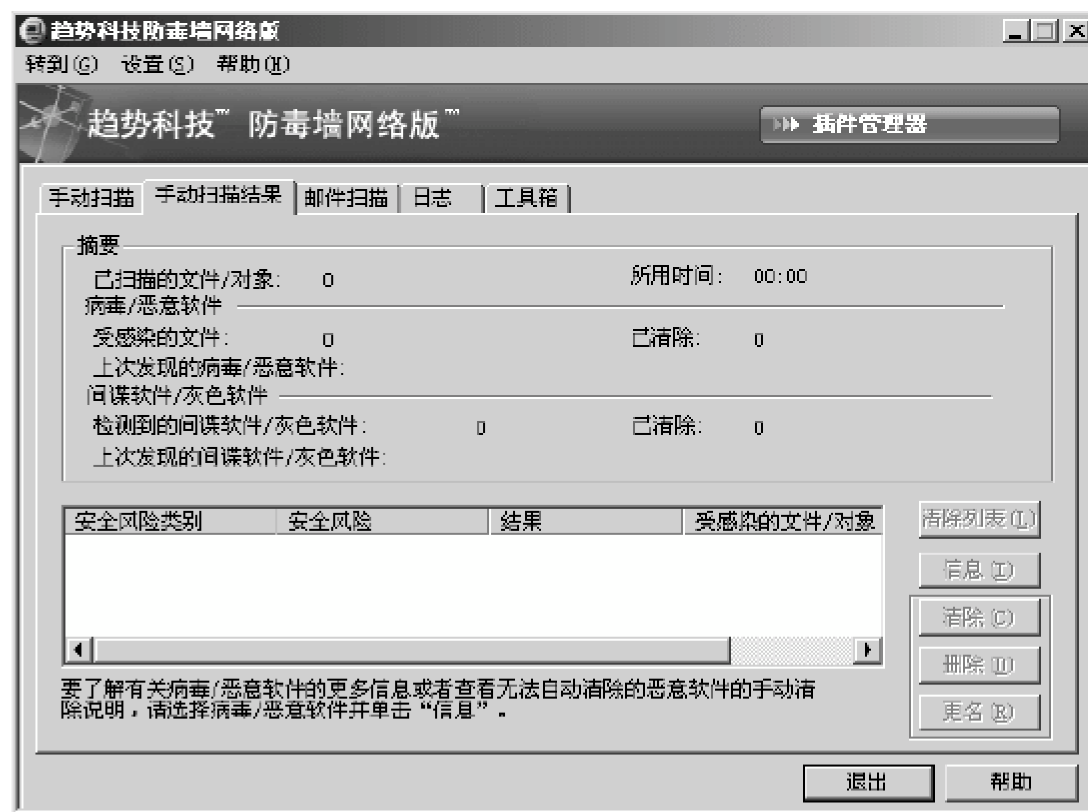


图 19-131　【手动扫描结果】选项卡

03 选择【邮件扫描】选项卡，在打开的界面中选中【从邮件服务器下载 POP3 邮件和附件时进行扫描】复选框，开启邮件扫描功能，如图 19-132 所示。

04 选择【日志】选项卡，在打开的界面中选择日志类型并指定日志范围，单击【查看日志】按钮，可以翻阅日志查找故障，如图 19-133 所示。



图 19-132 【邮件扫描】选项卡



图 19-133 【日志】选项卡



提 示

由于日志占用的空间会越来越大，用户可以单击【编辑】按钮进行日志维护。

19.4 专家答疑

（1）企业架设了反病毒系统，为什么还总是有大量病毒传播？

答：架设了反病毒系统后，没有达到病毒防护的原因有以下几点。首先，可能是企业网络感染了新的病毒，而病毒库没有得到及时更新，导致该病毒无法被发现。其次，架设企业反病毒系统时，必须要保证所有主机都处于企业反病毒系统中，如果部分新加主机没有配置反病毒客户端，很可能成为整个网络病毒肆虐的源头，即便网络管理员一再查杀，但是始终清除不了这些主机的安全隐患。再次，反病毒系统架设好之后，要配置合理的病毒查杀计划任务，并要定期手动全网查杀病毒，而且病毒查杀配置可以设置为深度扫描。最后，网络管理员需要规范员工的上网行为和计算机使用行为，从根源上减少计算机病毒流入网络。

（2）反病毒系统程序升级和病毒库更新总是出现失败，怎么办?

答：首先要强调的是反病毒程序升级和病毒库必须要及时更新，如果不能更新要及时解决问题。出现更新失败的主要原因有以下几点。首先，可能是程序的注册信息过期或错误，需要找客服询问，或到其产品官网更新注册信息。其次，可能是反病毒系统无法连接到更新服务器，可以查看其更新服务器的地址配置是否正确，如果不确定可以指定自动获得服务器地址或者到官网查询更新服务器地址。再次，本地网络连通性也会影响更新，可以使用 PING 命令检测服务器是否连通。最后，也有可能是系统服务冲突，需要进行详细的系统分析，但是一般不会出现冲突现象。

第 20 章　企业防火墙架设与使用

随着依赖网络、计算机办公的人和企业越来越多，相应的网络威胁也层出不穷，如常见的病毒、木马、网络攻击等。一旦企业网络和家庭个人计算机遭受网络威胁，对企业或个人都会带来巨大的损失，尤其是企业网络。目前解决外网攻击的最有力手段就是防火墙技术。

20.1　防火墙概述

大多数人都接触过防火墙技术，平时使用 Windows 系统时，为了安全个人主机通常会开启 Windows 自带的防火墙，以保护个人主机的安全。另外，局域网内往往会出现 ARP 病毒或攻击，使个人主机遭受地址欺骗，这时可以使用 ARP 防火墙阻止外部地址欺骗的攻击流，保护主机安全。但在复杂的企业网络环境中，网络攻击的数量、威胁都很大，一个单机防火墙根本解决不了全网的网络威胁，这时就需要使用企业防火墙。

20.1.1　企业防火墙

企业防火墙是指由软件和硬件设备构成的用于限制企业内网和外网之间流量访问的安全架构。防火墙是一种访问控制和隔离技术，是网络安全区域和不安全区域的屏障。

企业防火墙可以作为内网的安全网关，确保内网免受外网非法用户的入侵。防火墙可以通过服务访问规则、验证技术、包过滤和应用网关四部分功能，使流入流出的所有信息被检测和控制，所有具有安全隐患的流量都可以被拒绝通过防火墙转发。

在企业网内部，并不是每一个用户都能安全地使用计算机。大多数用户对计算机的安全配置了解甚少，经常出现不安装防火墙、杀毒软件，处于“裸奔”状态的主机，再加上有些用户上网行为不规范，很容易成为外网攻击者实施全网攻击的跳板。与逐个地督促和管理用户安全使用计算机相比，在网络出口架设一套防火墙系统显得更为有效。

企业防火墙并不是在网络出口位置安装了就能起到保护全网的作用，在架设防火墙系统时还应当设计一套安全、可靠的访问控制规则，准确地拒绝、过滤具有安全隐患的流量，而让合法的流量顺利通过。所以，一套完整的企业防火墙系统应当由两部分组成：软硬件防火墙环境和防火墙配置策略。

20.1.2 防火墙的分类

防火墙技术自出现，发展至今已经产生了很多类型。可以从功能、技术、结构、性能等多个方面面对防火墙进行分类，如表 22-1 所示。

表 22-1 防火墙的分类

分类方式	类别		
软硬件构成形式	软件防火墙	硬件防火墙	芯片级防火墙
防火墙功能技术	包过滤防火墙	状态检测防火墙	应用代理型防火墙
防火墙结构	单一主机防火墙	集成路由防火墙	分布式防火墙
防火墙的应用部署位置	边界防火墙	个人防火墙	混合防火墙
防火墙性能	百兆级防火墙	千兆级防火墙	
防火墙使用方法	网络层防火墙	物理层防火墙	链路层防火墙

防火墙的种类繁多，选择防火墙考虑最多的还是其功能技术。下面介绍一下包过滤防火墙、状态检测防火墙和应用代理型防火墙。

1. 包过滤防火墙

包过滤防火墙将对每一个接收到的包进行分析，通过匹配过滤规则，做出允许或拒绝的决定。过滤规则匹配的主要是 IP 数据报的报头信息，包括源 IP 地址、目的 IP 地址、协议类型（TCP 包、UDP 包、ICMP 包）、源端口、目的端口等报头信息。当数据包通过防火墙时，会逐个检测每一条规则，一旦有信息匹配成功，就会按照过滤规则进行转发或者丢弃。如果没有规则和数据包匹配，防火墙会采用默认规则，一般默认丢弃所有不匹配数据包。

包过滤防火墙需要处理数据包的 IP 信息和 TCP/UDP 信息来匹配规则，所以它工作在网络层和传输层。和代理服务器相比，它只需要将数据包拆到第四层，处理速度要快一些。它对于网络攻击单一、威胁一般的中小网络比较适用，而对于基于应用层的威胁不能做出反应，所以在安全级别较高的网络不建议选择。同时包过滤防火墙在价格上一般比代理防火墙便宜，适合中小企业使用。

包过滤防火墙也存在很多问题。首先，它只能过滤到端口，却无法分析数据内容，利用安全端口隐藏攻击的数据包无法过滤。其次，在网络环境比较复杂的情况下，网络管理员需要配置的访问规则将会很复杂，不利于管理。

2. 状态检测防火墙

状态检测防火墙是传统包过滤防火墙的功能扩展，除了有包过滤功能外，还可以抽取数据包和应用层状态相关的信息，并以此为依据决定是否允许数据包通过。能够实现该功能主要是依靠状态检测防火墙内部有一个不需要配置、自动产生的状态表。状态表规定了允许的源 IP 地址和目的 IP 地址、源端口和目的端口、数据包的 TCP 序列号和标志位等信息。

状态检测防火墙除了具有包过滤防火墙的优点外，对应用是透明的，而且在安全性上做了较大幅度的提升。防火墙接收到数据包后，首先会逐个检测过滤策略，如果没有策略允许通过，该数据包被丢弃，如果有允许策略匹配，数据包将被接受，并建立连接状态，后续数据包以此连接状态为标准进行匹配，一致则被转发，不一致则被丢弃。

整体来看，状态检测防火墙具有安全性高、性能好、扩展性好、配置方便等优点，所以这类

防火墙应用比较广泛。但是状态检测防火墙和包过滤防火墙一样，依然只是检测数据包的网络层和传输层信息，不能分析更高层次的数据，对于隐藏在应用层的攻击无法进行阻止。

3. 应用代理型防火墙

应用代理型防火墙也叫应用层网关防火墙。这种防火墙通过在 TCP 连接中加入一种 Proxy（代理）技术的方式实现安全隔离。从网络内部发出的数据包，在经过防火墙后，会被处理成以防火墙外部网卡为源的数据包，这样可以达到隐藏内网环境的作用。

应用代理型防火墙在实现代理转发的过程中，会对数据包的应用层数据作出分析，安全级别远远高于前两种防火墙。目前为止这类防火墙也是公认的最安全的防火墙。

20.1.3　防火墙联网模型

有了防火墙之后，又当如何连接呢？这是在防火墙部署过程中最重要的设计内容。直接影响到整个网络的应用和安全性。下面详细介绍三种常用的防火墙联网模型。

1. 双向边缘防火墙联网模型

这类防火墙联网模型比较简单，只要防火墙具备两个接口就可以实现，通常适用于中小企业，如图 20-1 所示。

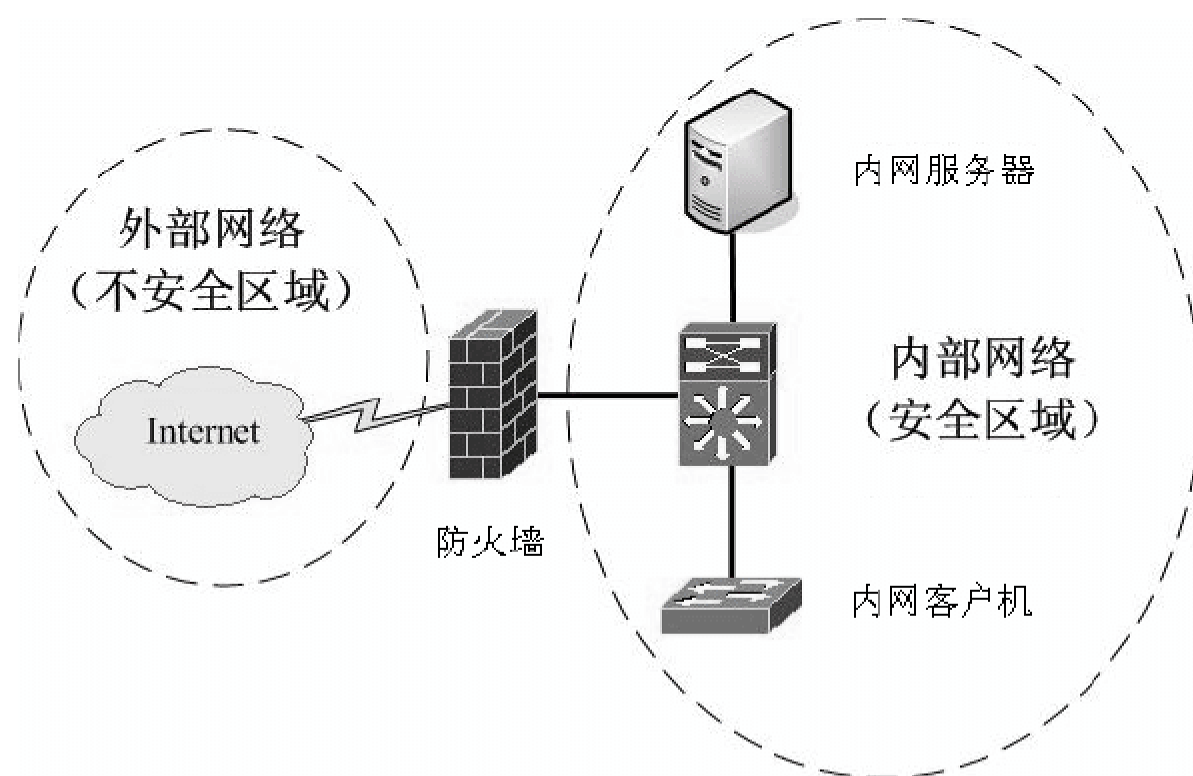


图 20-1　双向边缘防火墙联网模型

2. 带有 DMZ 区的 3 向防火墙联网模型

这类防火墙联网模型在双向边缘防火墙基础上增加了一个独立的 DMZ（隔离区），该区域用于放置对外网公开发布的服务器，如企业 Web 服务器、邮件服务器等，如图 20-2 所示。DMZ 区的意义在于，当外部网络访问企业网站时，只能访问到 DMZ 区，而不能访问内部网络，相比把服务器和内网客户机放置在同一区域安全了很多，相当于一个外部不安全区域和内部安全区域的缓冲区。通过这样一个 DMZ 区域，更加有效地保护了内部网络的安全。

部署这类防火墙联网模型比较复杂，防火墙本身必须支持 DMZ 区功能并且有可用的 DMZ 接口，如果是软件防火墙，系统平台也至少要有三个网卡接口。

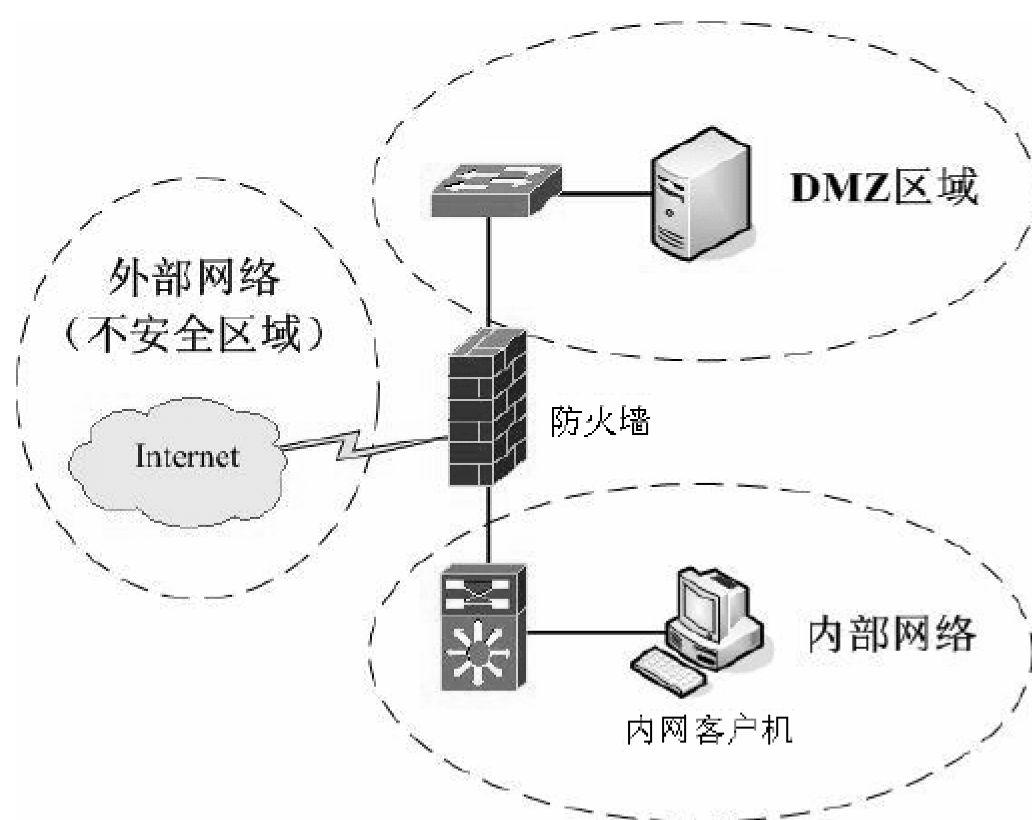


图 20-2　带有 DMZ 区的 3 向防火墙联网模型

3. 前后端防火墙联网模型

前后端防火墙联网模型和带有 DMZ 区的 3 向防火墙联网模型比起来略有些复杂，将 DMZ 区独立于两个防火墙之间，如图 20-3 所示。这样部署会使内部的安全网络和外部的不安全网络实现物理隔离，更好地保证内外网通信安全。

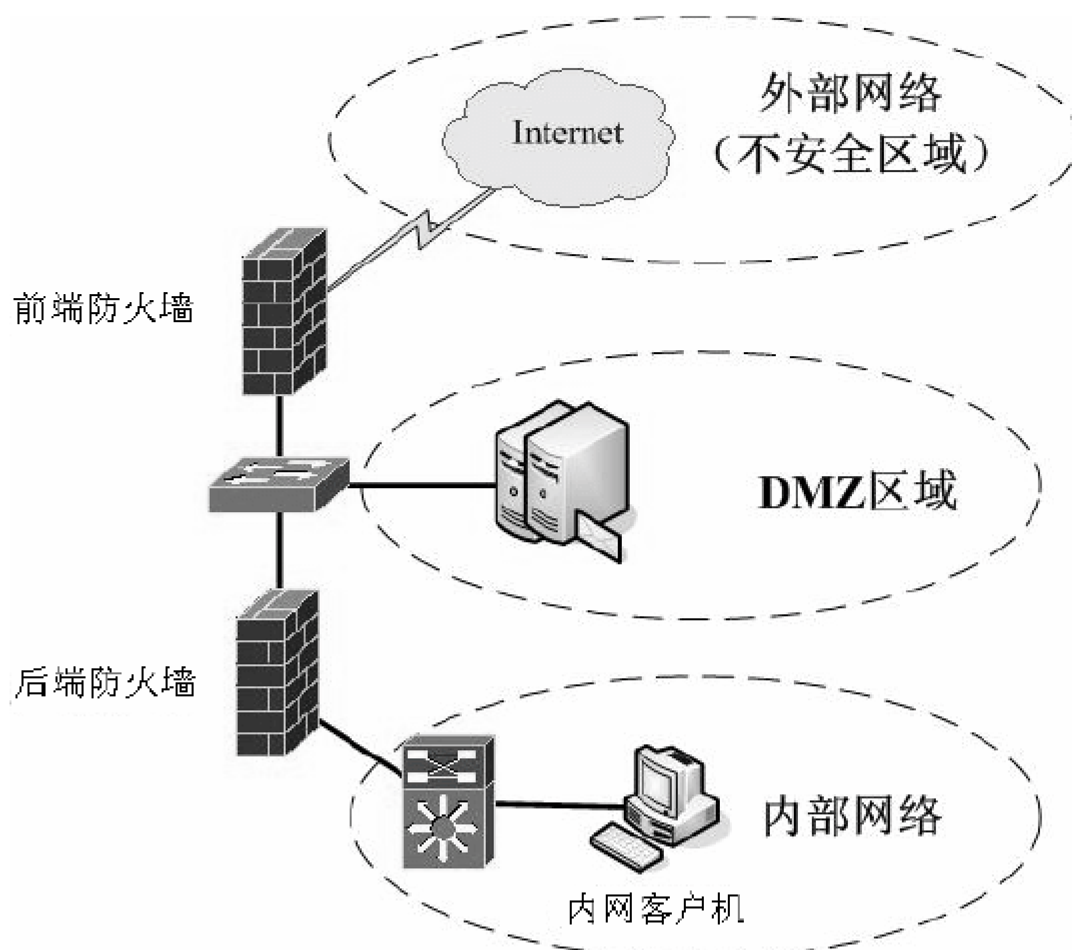


图 20-3　前后端防火墙联网模型

4. 高可用的防火墙联网模型

高可用的防火墙联网模型由两个防火墙同时进行隔离、过滤、转发工作，如图 20-4 所示。通信工作由两个防火墙分担进行，提高了工作效率。如果有一个防火墙出现了故障，另一个防火墙依然可以正常工作，提高了网络的可用性。这类防火墙联网模型一般适用于对性能和可用性要求比较高的大中型网络和一些特殊的中小型网络。

这类防火墙联网模型部署起来相对比较复杂，不但在配置上比较复杂，对设备的硬件要求也比较高，特别是接口数量，需要有足够的接口做冗余连接。

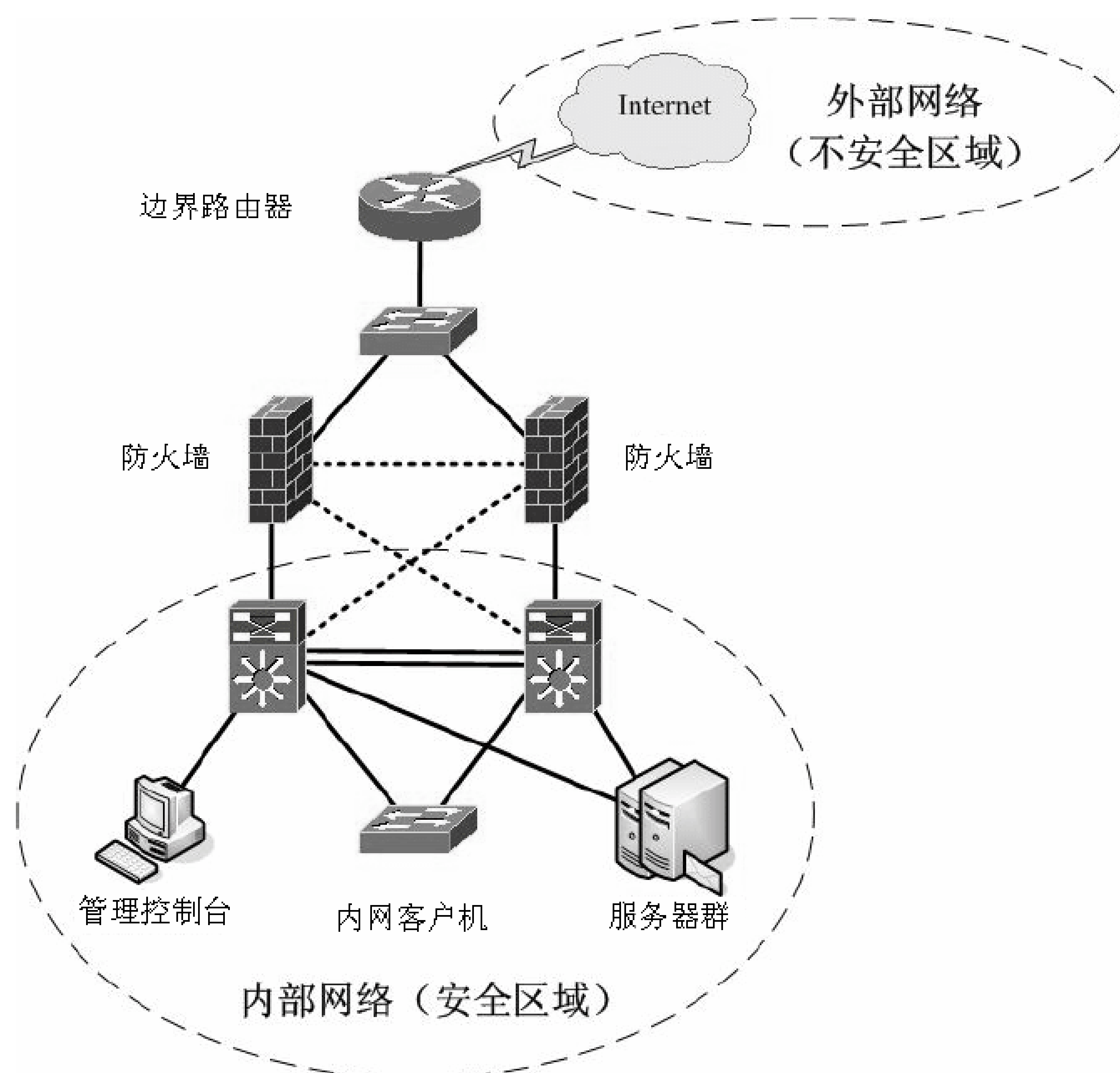


图 20-4 高可用的防火墙联网模型

20.1.4 产品选型

企业防火墙在网络环境的安全管理系统中分量很重，一般的企业在设计网络安全方案时，首先考虑的就是增加防火墙。但是不同的企业，选择防火墙时要有所差异。防火墙并不是越高端就越好，需要结合网络的自身情况来考虑，涉及的因素有以下几点。

1. 类型

防火墙有很多分类，有硬件防火墙、软件防火墙、代理防火墙、包过滤防火墙等多种类别，首先要选择的就是类型。一般中小企业使用最多的是包过滤防火墙和状态检测防火墙，代理防火墙在安全性要求较高的大型网络使用得比较多。

2. 性能

不同的产品其性能差异很大，一般硬件防火墙比软件防火墙在性能稳定性上要好很多，因为硬件防火墙不会受系统漏洞的影响。同时选择时应注意大厂商的产品稳定性性能发挥比小牌企业好很多。

除此之外，还要比较其性能参数是否符合企业需求，主要性能指标有过滤方式、地址绑定、访问控制、代理服务、带宽支持、地址转换、日志功能、路由功能、认证功能、邮件认证等。

3. 联网模型

根据企业业务需求，可能会实施不同的联网模型，而并不是所有防火墙都可以支持各类联网模型的使用，如果要架设双核心高可用性防火墙模型的话，防火墙的网络接口数量要求很多，例如需要架设带 DMZ 区的 3 向防火墙，就必须能支持 DMZ 功能。

4. 网络管理水平

选择防火墙时还需要考虑当前网络管理员的管理能力，并不是品牌好、性能好、服务好就能起到作用，还需要网络管理员使用好。有些防火墙配置起来需要较高的技术水平，如 Cisco 的 ASA 防火墙，如果不了解其应用原理和配置命令则操作起来很难。而 ISA Server 2006 软件防火墙，虽然没有 ASA 高端，但是其 Windows 系统下的全中文窗口配置界面环境管理员很容易操作。

5. 价格

其实有些企业在选择防火墙时考虑价格因素比较多，虽然碍于企业经济实力不得不考虑，但是最好将其放到最后一位。如果一个小企业的所有业务都和服务器的应用程序和数据库有关，一味地顾虑价格很可能降低数据的安全性保障。

通常使用比较多的防火墙有 ISA Server 2006、Cisco ASA、天融信、H3C、飞塔、启明星辰等。如果使用软件防火墙可以用 ISA Server 2006，如果是硬件防火墙可以考虑国产的几款产品。

20.2 项目实战 1：架设 ISA 企业防火墙

ISA Server 2006 防火墙是微软的防火墙，很多中小企业都在使用。下面详细介绍 ISA 企业防火墙的环境搭建与配置。

20.2.1 模拟企业网络搭建实验环境

ISA 企业防火墙是安装在 Windows 系统内的软件防火墙，下面在 Windows Server 2003 环境下搭建其模拟实验环境。

1. ISA 企业防火墙安装配置要求

ISA 防火墙处于网络的关键位置，需要保证其运行环境的稳定性，所以需要服务器满足一定的配置要求，详细配置要求如表 20-2 所示。

表 20-2 ISA 防火墙安装配置要求

组件	配置要求
操作系统	Windows Server 2003 32 位操作系统
处理器	装有 733MHz Pentium III 或更高的处理器
硬盘	至少 150MB 可用空间，分区为 NTFS 格式分区；运行时需要更多额外空间保存 Web 高速缓存等内容
内存	至少 512MB，建议使用更大容量
其他	网络适配器根据联网模型进行配备，键盘、显示器、鼠标、光驱等普通配置即可


提 示

以上配置要求只是最低性能标准，如果网络通信业务量比较大，建议使用更高的系统配置。

2. ISA 企业防火墙环境部署

在介绍 ISA 企业防火墙的配置内容时，以图 20-5 所示的联网方式进行讲解，主要由四台虚拟机进行模拟实验。

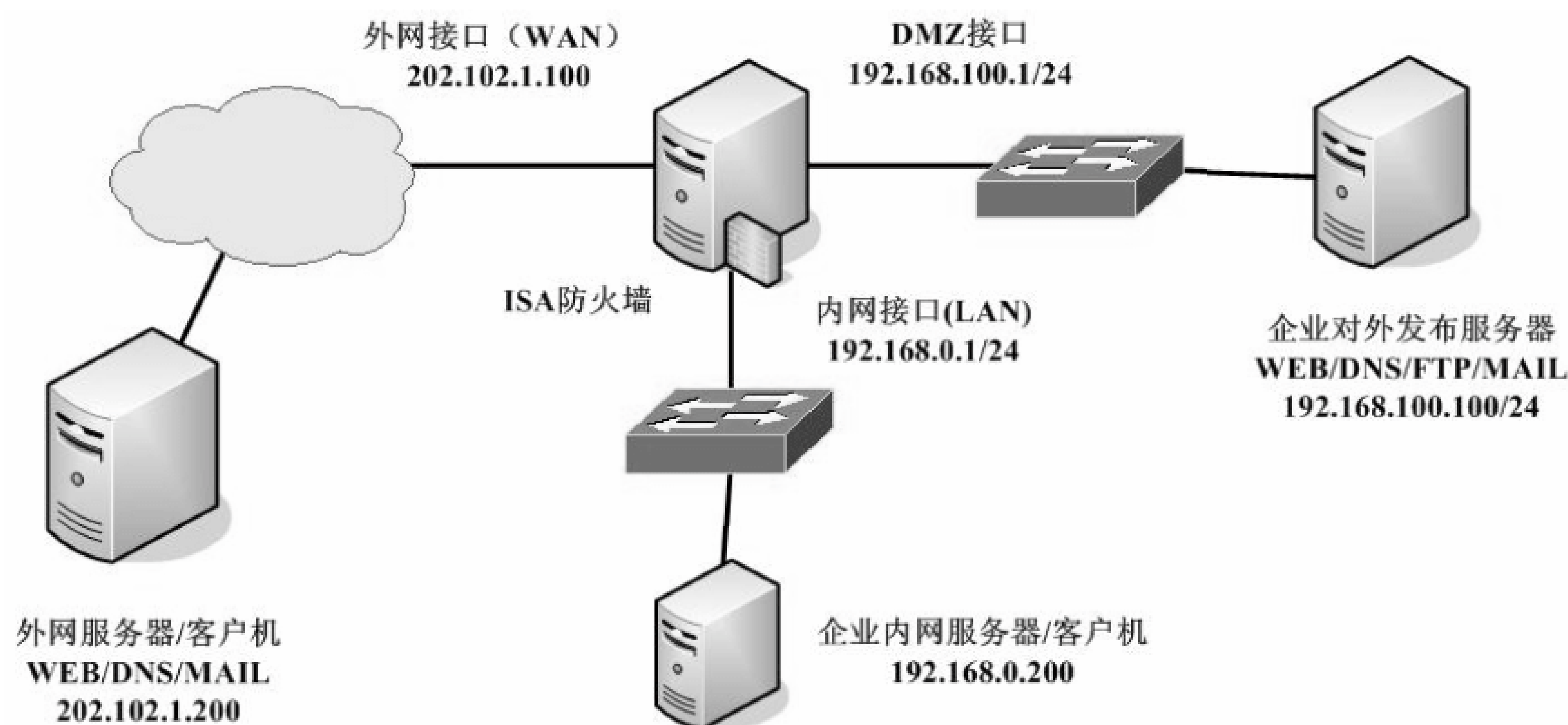


图20-5　ISA防火墙模拟实验拓扑图



提　示

本实例只做 ISA 企业防火墙的配合，内网、外网、DMZ 区的服务器和客户机不做配置讲解。

20.2.2　安装 ISA Server 2006 防火墙

在使用 ISA Server 2006 防火墙之前，需要先安装其应用程序，具体的操作步骤如下。

01 将 ISA Server 2006 安装光盘放入光驱内，系统读取光盘内容，弹出【Microsoft ISA Server 2006 安装程序】窗口，单击【安装 ISA Server 2006】链接，如图 20-6 所示。

02 弹出【欢迎使用 Microsoft ISA Server 2006 的安装向导】对话框，单击【下一步】按钮，如图 20-7 所示。

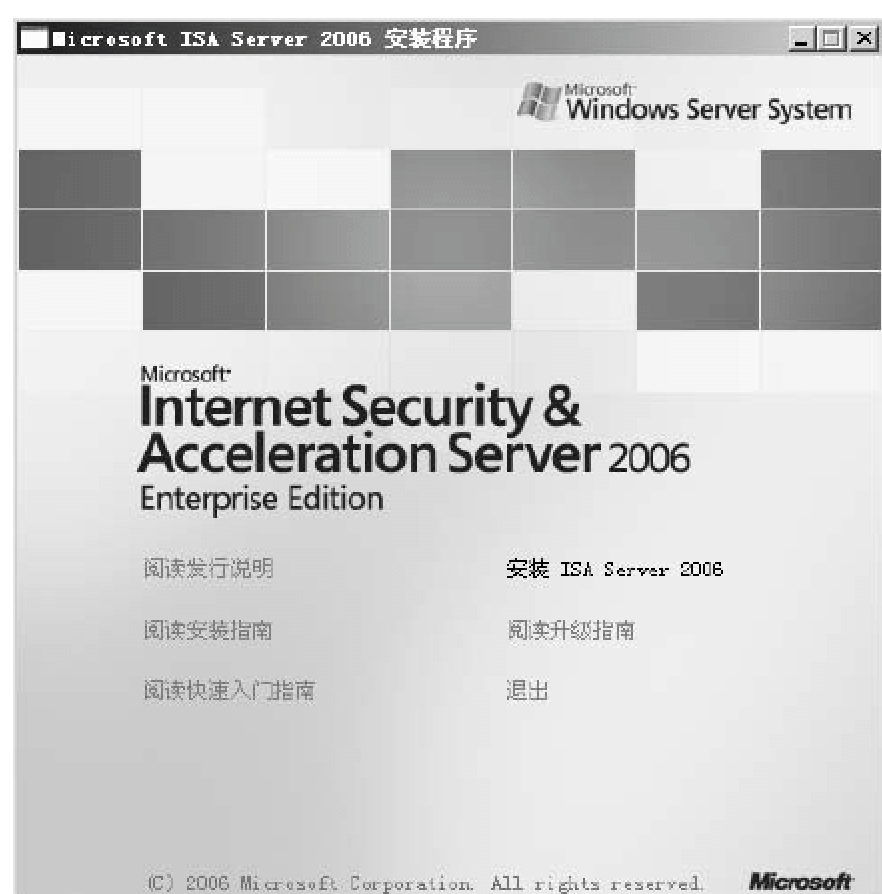


图 20-6　【Microsoft ISA Server 2006 安装程序】窗口



图 20-7　ISA Server 2006 安装向导

03 弹出【许可协议】对话框，选中【我接受许可协议中的条款】单选按钮，单击【下一步】按钮，如图 20-8 所示。

04 弹出【客户信息】对话框，在其中输入匹配信息及产品序列号，单击【下一步】按钮，如图 20-9 所示。



图 20-8 【许可协议】对话框



图 20-9 【客户信息】对话框

05 弹出【安装方案】对话框，选中【同时安装 ISA Server 服务和配置存储服务器】单选按钮，单击【下一步】按钮，如图 20-10 所示。

06 弹出【组件选择】对话框，默认选择安装所有组件，单击【更改】按钮，可以改变程序的安装目录位置，本实例采用默认配置，如图 20-11 所示，单击【下一步】按钮。

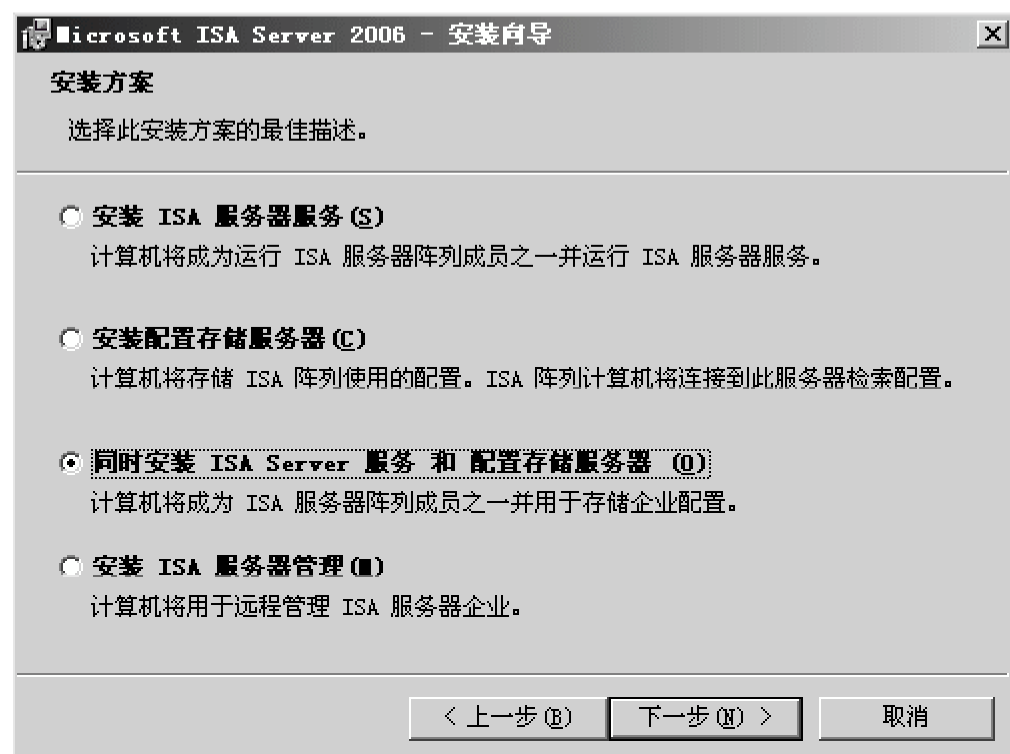


图 20-10 【安装方案】对话框

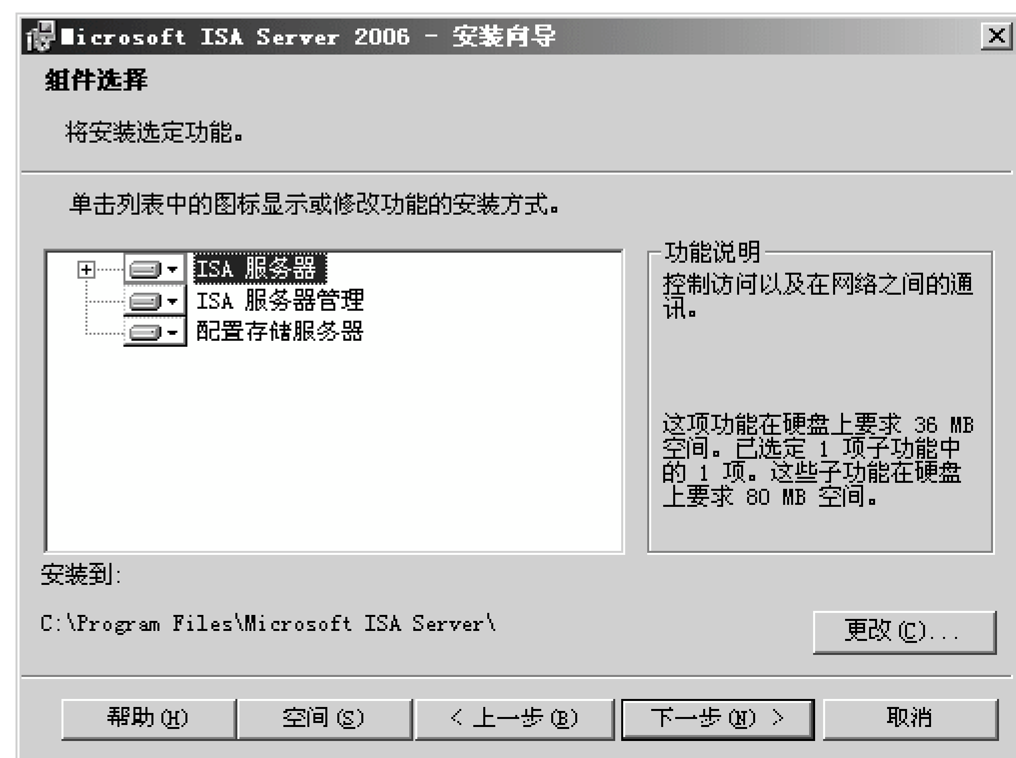


图 20-11 【组件选择】对话框

07 弹出【企业安装选项】对话框，由于初次搭建 ISA 防火墙，所以选中【创建新 ISA 服务器企业】单选按钮，如图 20-12 所示，单击【下一步】按钮。

08 弹出【新建企业警告】对话框，如图 20-13 所示，单击【下一步】按钮。

09 弹出【内部网络】对话框，单击【添加】按钮，指定 ISA 内部网络的地址范围，如图 20-14 所示。

10 弹出【地址】对话框，可以单击【添加适配器】按钮指定内部网卡，也可以单击【添加范围】按钮指定内部网络地址范围，本实例选择指定内部网卡，如图 20-15 所示。

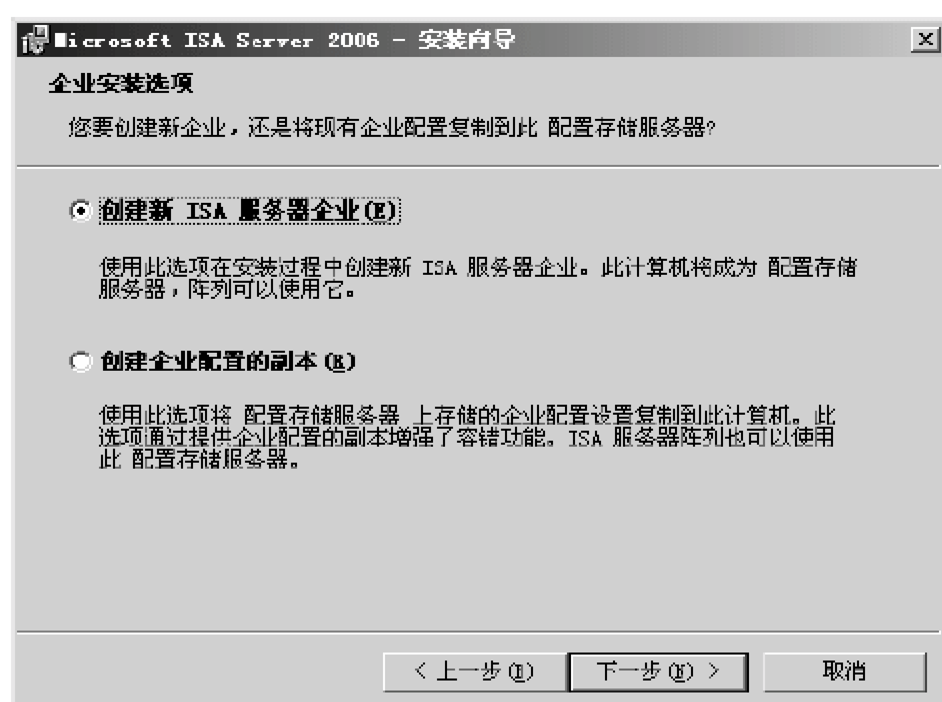


图 20-12　【企业安装选项】对话框

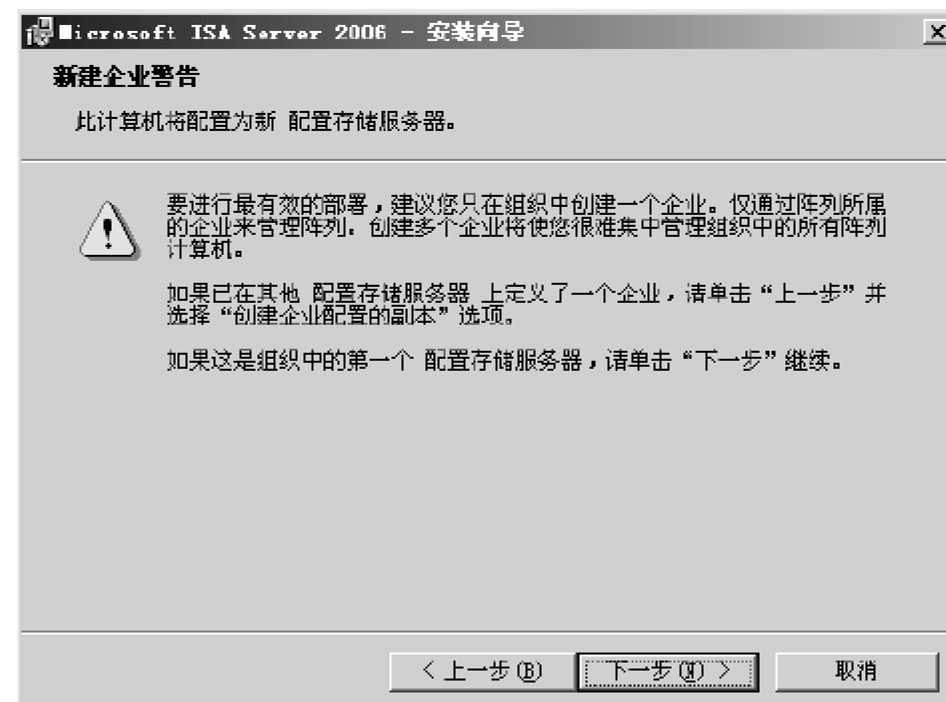


图 20-13　【新建企业警告】对话框



图 20-14　【内部网络】对话框

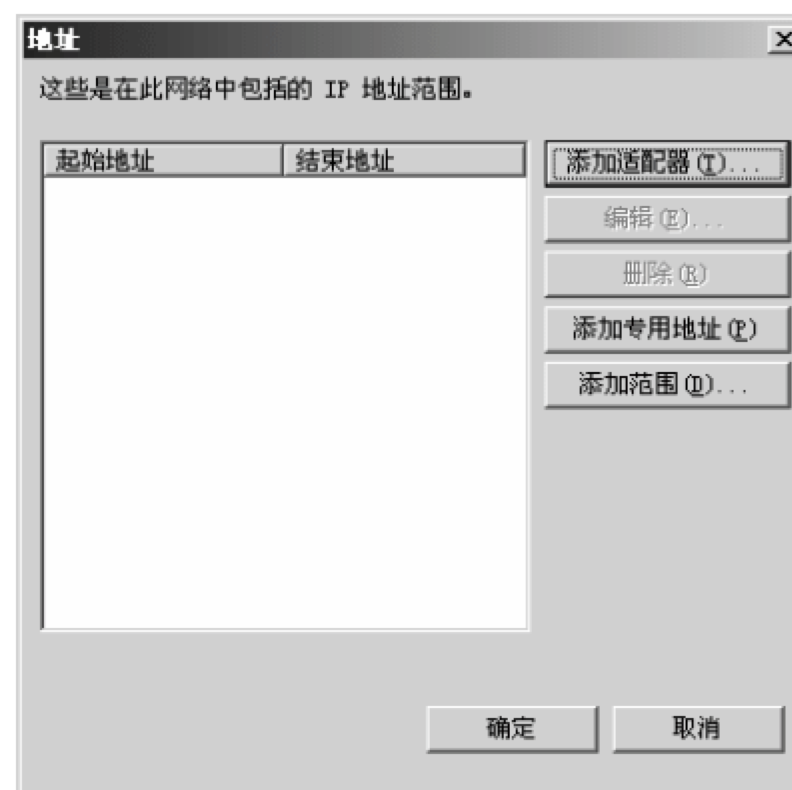


图 20-15　【地址】对话框

11 弹出【选择网络适配器】对话框，在【网络适配器】列表框中显示了服务器的三块网卡，选中 LAN 复选框，在【网络适配器详细信息】列表中显示出 LAN 网卡的详细信息，单击【确定】按钮，如图 20-16 所示。

12 返回【地址】对话框，如图 20-17 所示，地址范围添加完成，单击【确定】按钮。

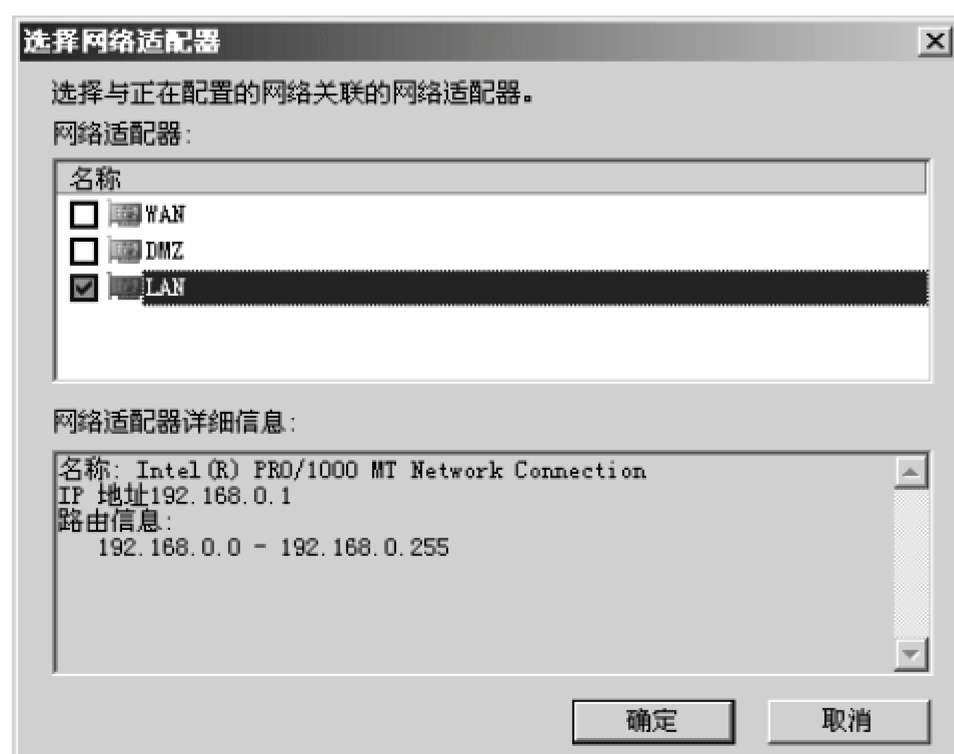


图 20-16　【选择网络适配器】对话框

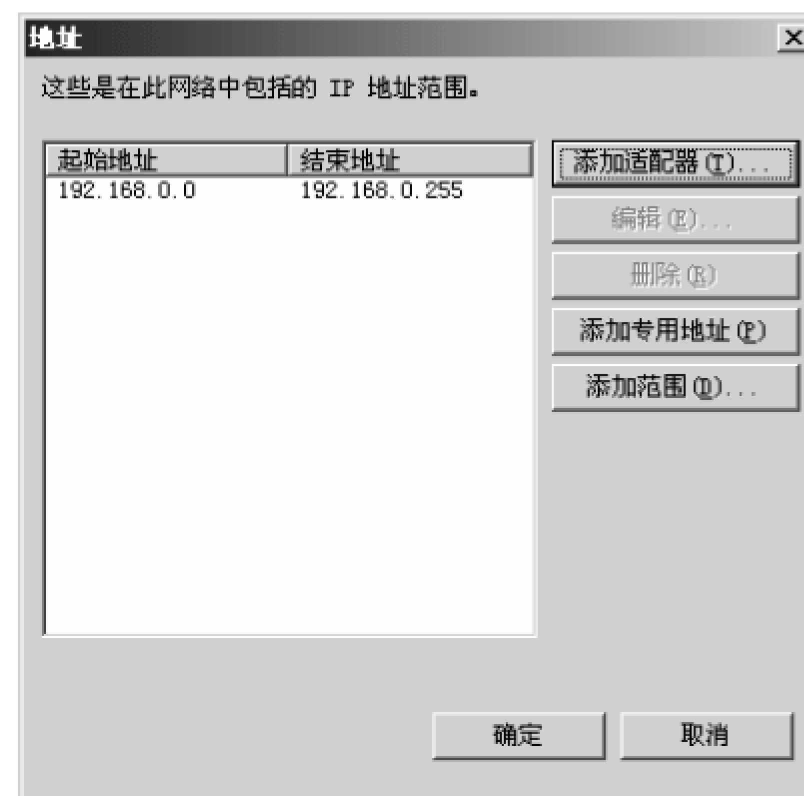


图 20-17　【地址】对话框

13 返回【内部网络】对话框，如图 20-18 所示，在【内部网络地址范围】列表框中显示内部地址范围，单击【下一步】按钮。

14 弹出【防火墙客户端连接】对话框，如图 20-19 所示，该对话框主要设置 ISA 对旧版本系统客户端的兼容，本实例采用默认配置，单击【下一步】按钮。



图 20-18 【内部网络】对话框

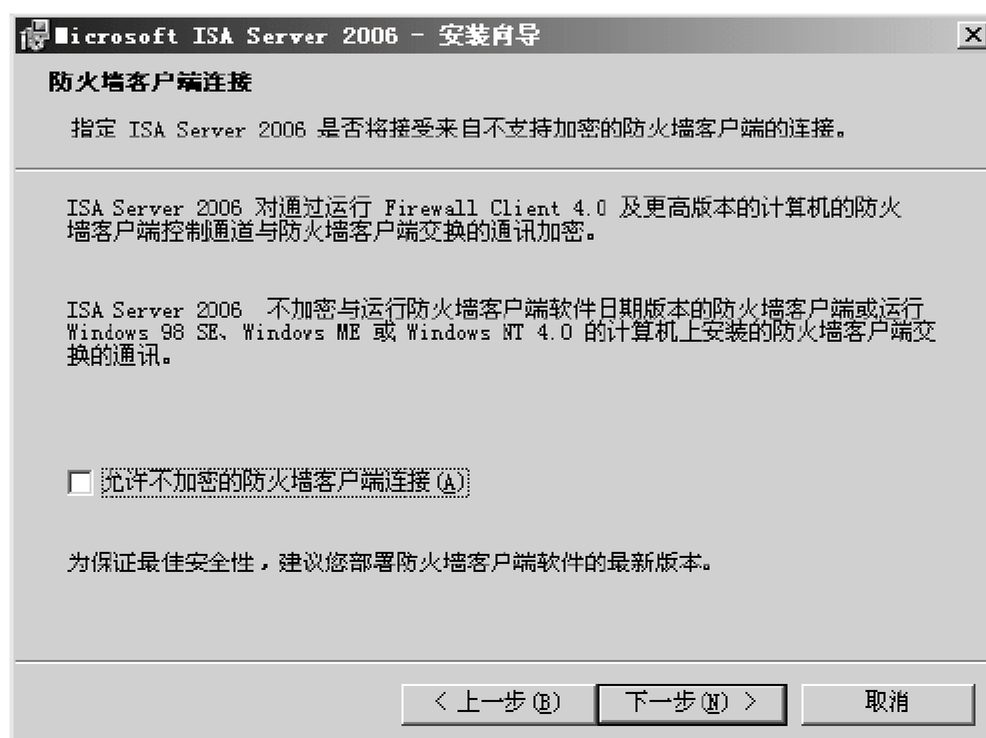


图 20-19 【防火墙客户端连接】对话框

15 弹出【服务警告】对话框，如图 20-20 所示，部分系统程序会影响 ISA 程序的安装，需要在安装 ISA 时将这些服务重新启动，单击【下一步】按钮。

16 弹出【可以安装程序了】对话框，如图 20-21 所示，单击【安装】按钮。

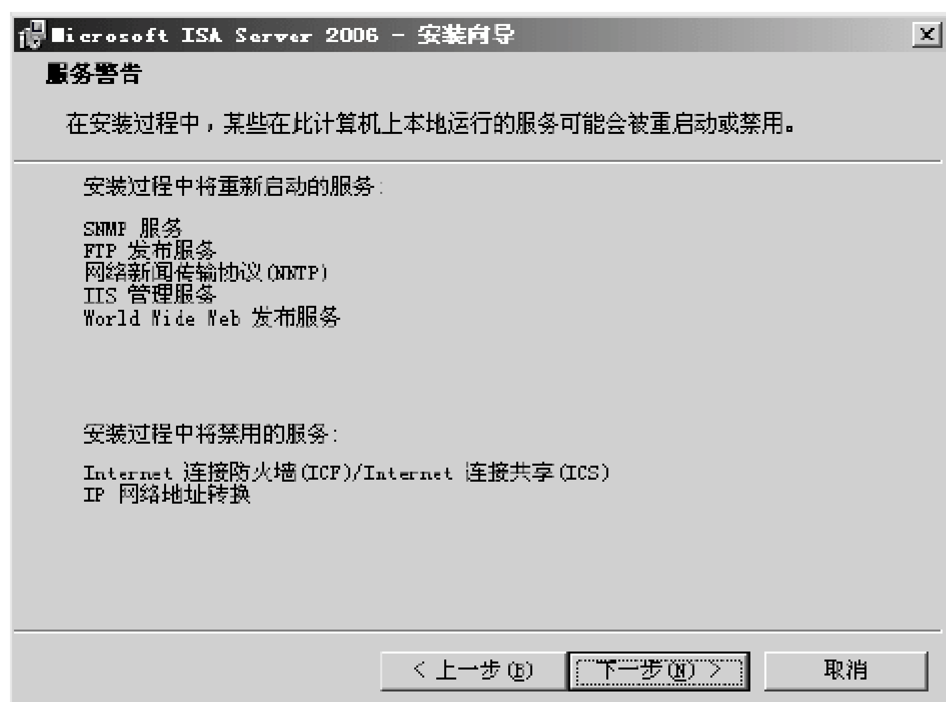


图 20-20 【服务警告】对话框

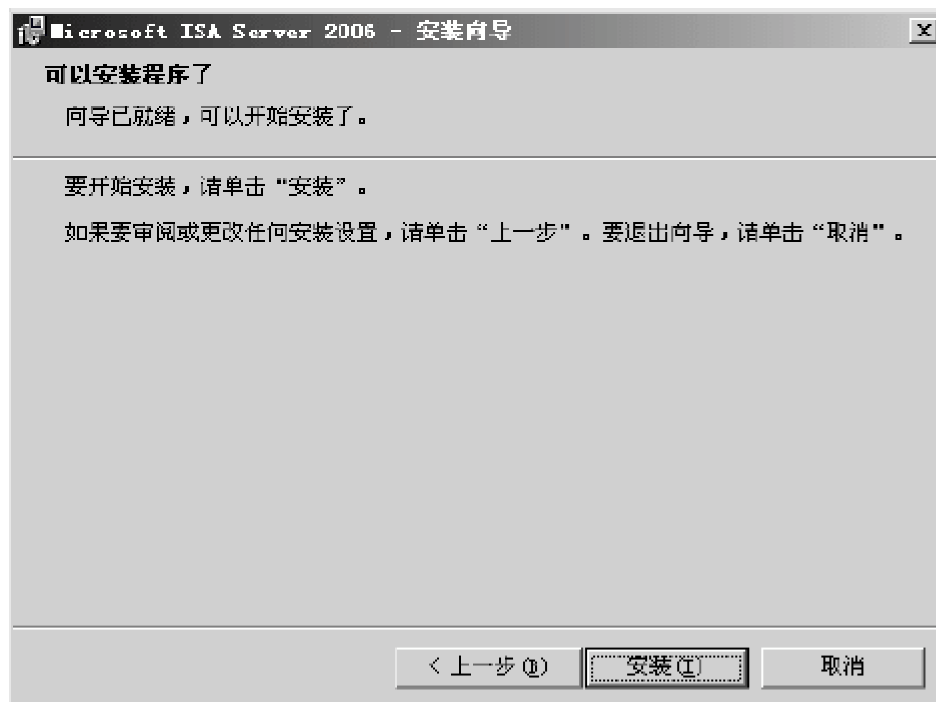


图 20-21 【可以安装程序了】对话框

17 系统依照配置自动安装程序，安装完成后弹出【安装向导完成】对话框，如图 20-22 所示，单击【完成】按钮，至此 ISA 2006 已经安装成功。



图 20-22 【安装向导完成】对话框

20.2.3　添加 DMZ 区，改变 ISA 联网模式

DMZ 区作为对外发布服务器的位置，需要连入 ISA 防火墙，但是默认安装完 ISA 防火墙，没有添加 DMZ 区的网卡，想要把 DMZ 区网络加入 ISA 防火墙，需要手工添加。

添加 DMZ 区域的具体操作步骤如下。

01 选择【开始】➢【程序】➢ Microsoft ISA Server ➢【ISA 服务器管理】命令，运行 ISA 防火墙，如图 20-23 所示。

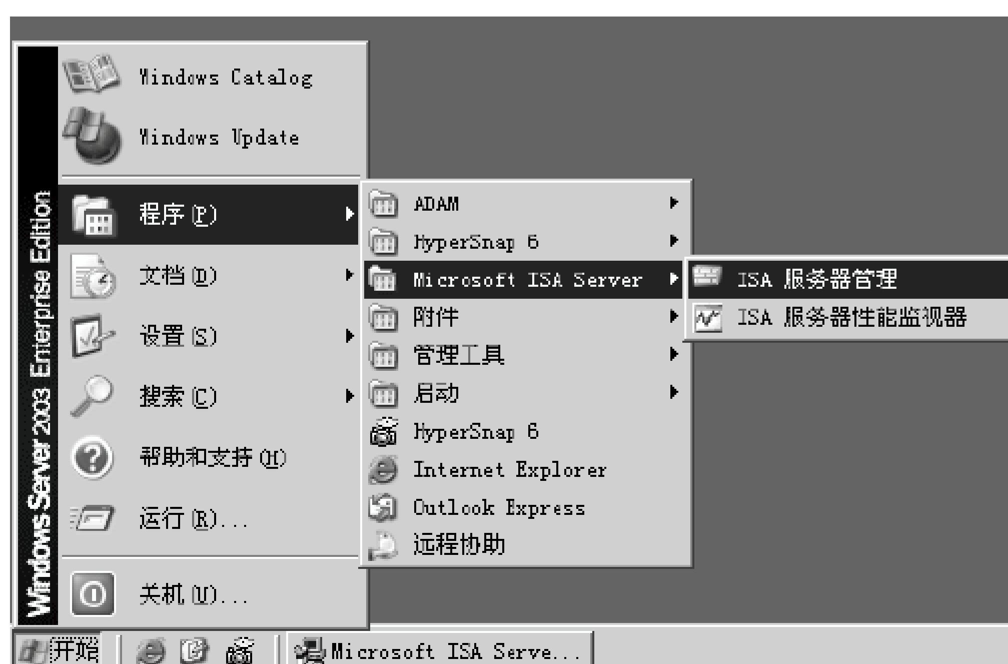


图 20-23　【IAS 服务器管理】选项

02 打开程序主界面，如图 20-24 所示，在左侧选项列表中选择【阵列】➢ aa-6db32af13796 ➢【配置】➢【网络】选项，aa-6db32af13796 为本地服务器计算机名，右侧显示出当前 ISA 防火墙采用的是【边缘防火墙】部署结构，在右侧【模板】选项卡中显示了可用 ISA 部署结构，选择【3 向外围网络】选项。



图 20-24　ISA Server 2006 程序窗口

03 弹出【网络模板向导】对话框，如图 20-25 所示，单击【下一步】按钮。

04 弹出【导出 ISA 服务器的配置】对话框，如图 20-26 所示。如果担心当前 ISA 服务器丢失，可以单击【导出】按钮将现有配置导出保存，单击【下一步】按钮。



图 20-25 【网络模板向导】对话框

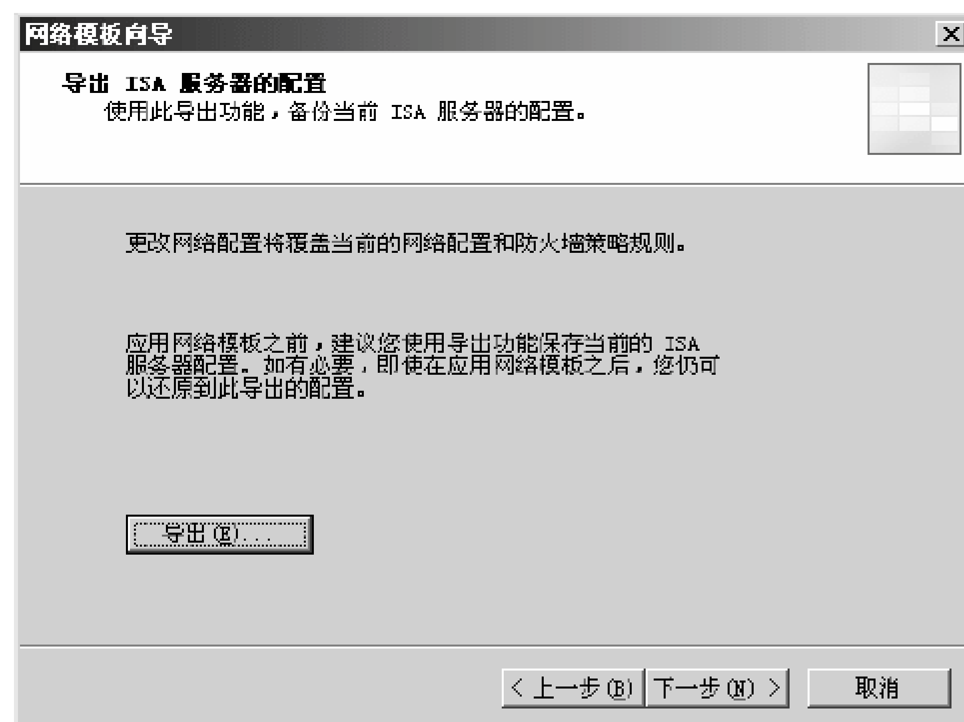


图 20-26 【导出 ISA 服务器的配置】对话框

05 弹出【内部 网络 IP 地址】对话框，如图 20-27 所示。安装防火墙时此项配置已经操作，单击【下一步】按钮。

06 弹出【外围 网络 IP 地址】对话框，如图 20-28 所示。“外围网络”就是“DMZ 区”，单击【添加适配器】按钮。

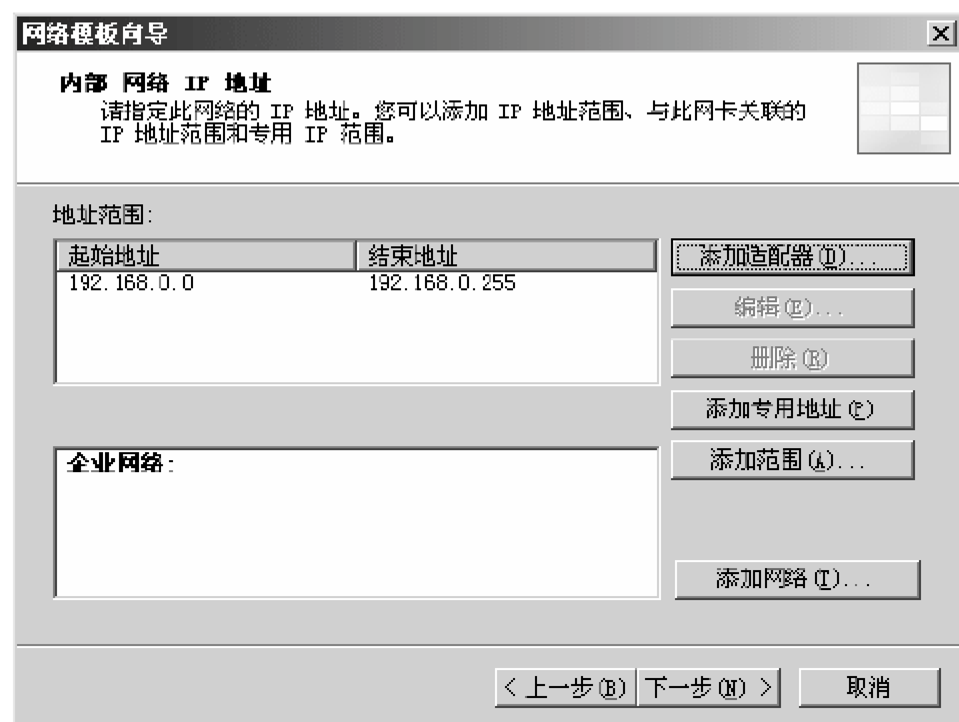


图 20-27 【内部 网络 IP 地址】对话框

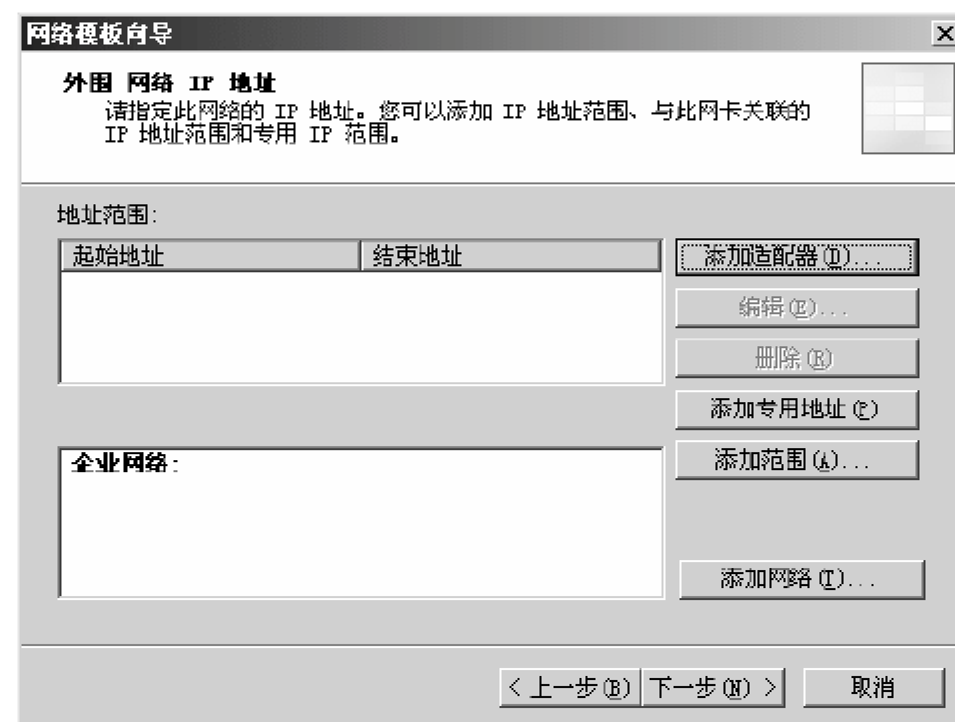


图 20-28 【外围 网络 IP 地址】对话框

07 弹出【选择网络适配器】对话框，如图 20-29 所示，在【网络适配器】选项列表框中选中 DMZ 复选框，单击【确定】按钮。

08 返回【外围 网络 IP 地址】对话框，如图 20-30 所示，在【地址范围】列表框中已显示 DMZ 区的网络地址范围，单击【下一步】按钮。

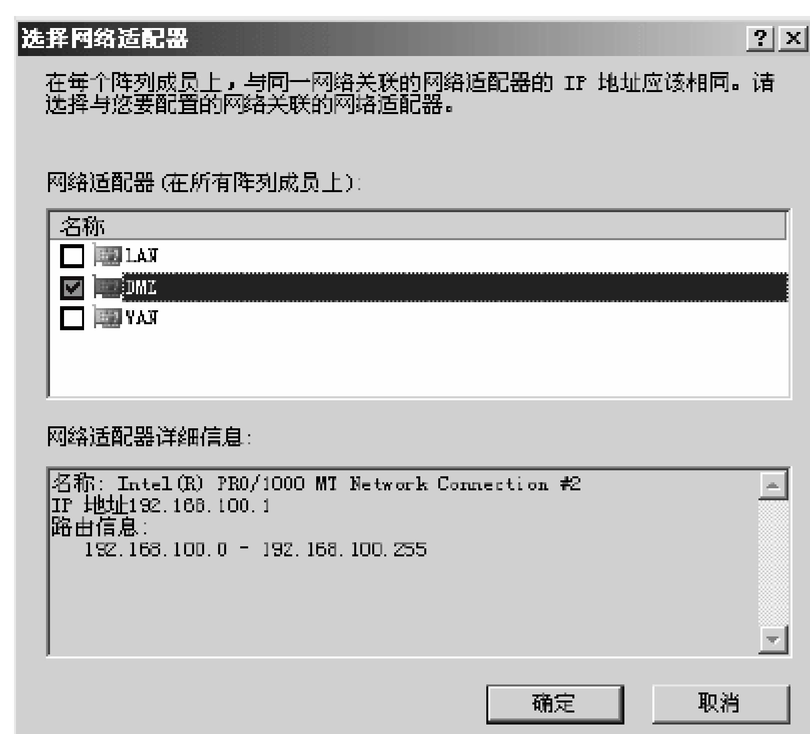


图 20-29 【选择网络适配器】对话框

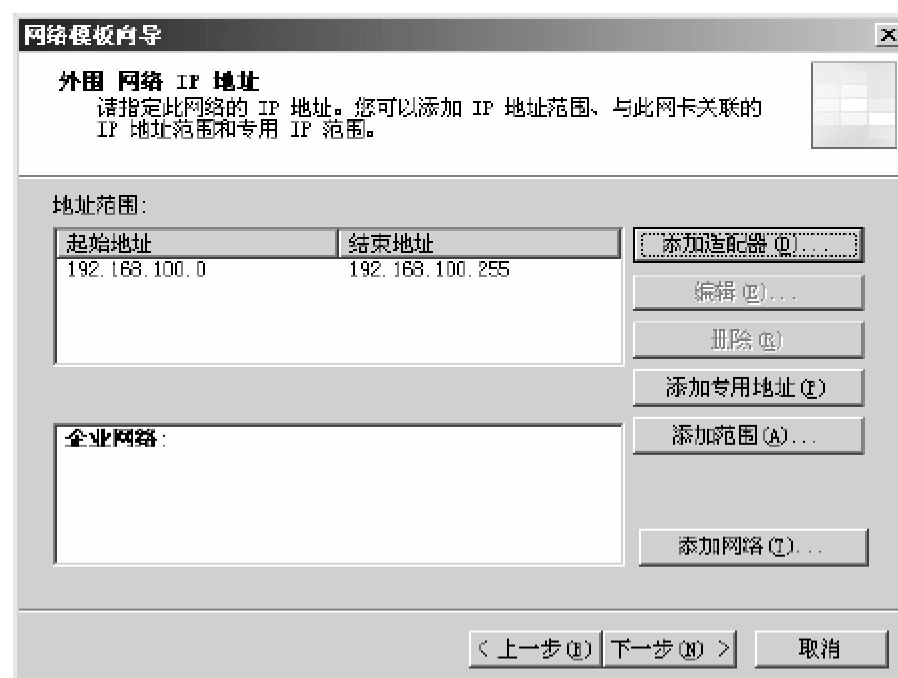


图 20-30 显示网络地址范围

09 弹出【选择一个防火墙策略】对话框，如图 20-31 所示，在此可以选择防火墙默认使用的控制策略，一般选择【阻止所有访问】，单击【下一步】按钮。

10 配置完成，在弹出的对话框中显示了新 ISA 部署结构的配置信息，如图 20-32 所示，单击【完成】按钮。

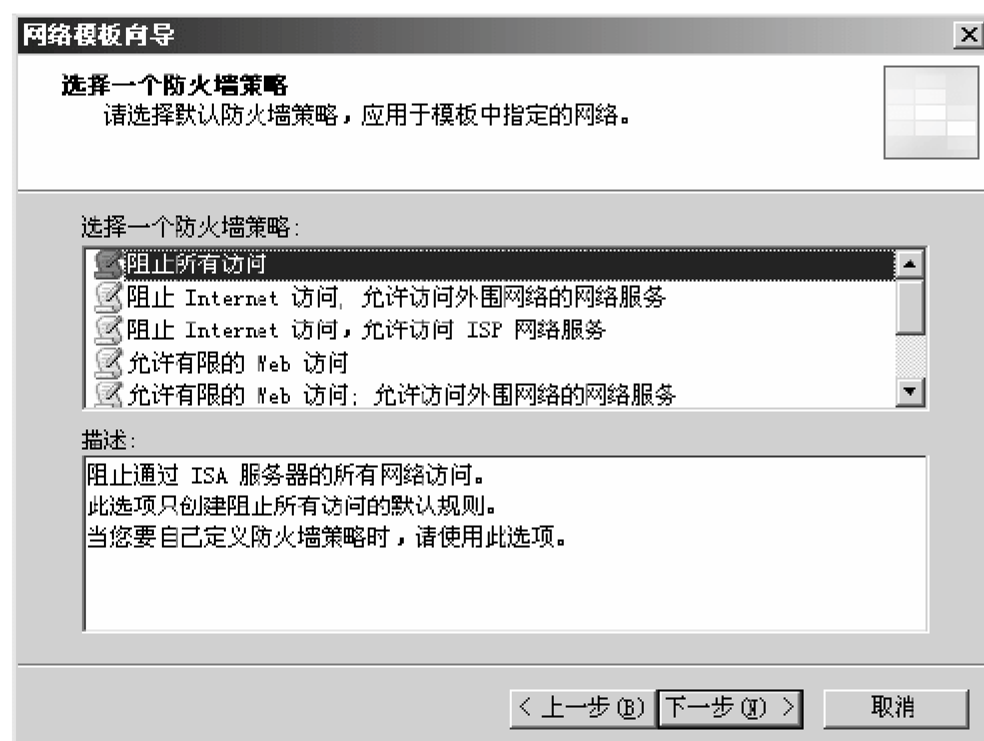


图 20-31 【选择一个防火墙策略】对话框

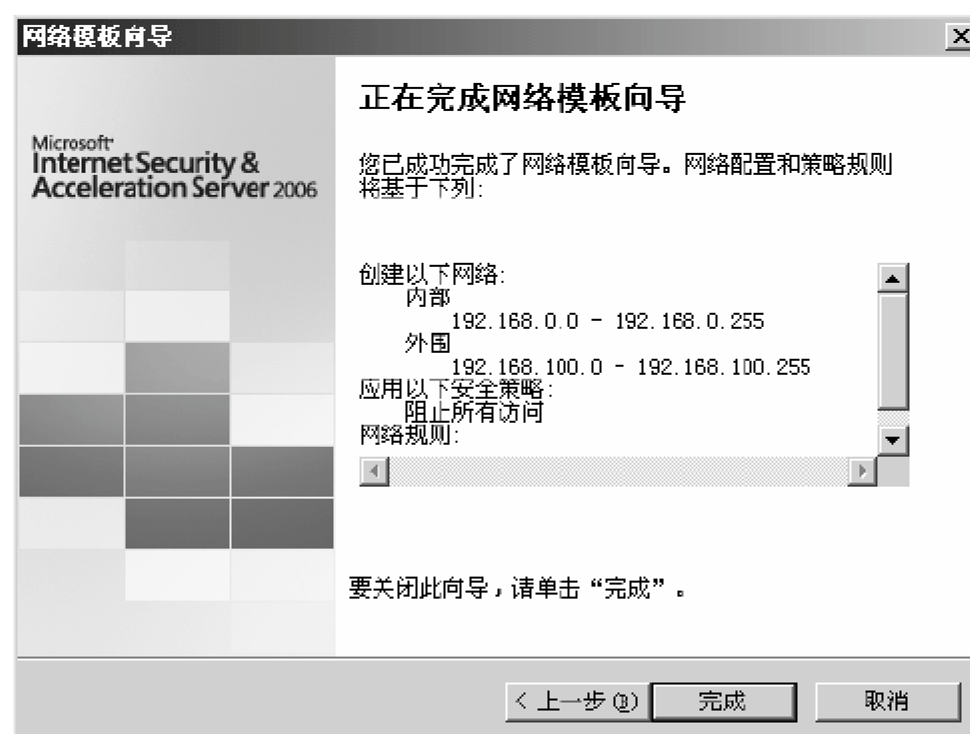


图 20-32 向导配置完成对话框

11 ISA 程序主界面显示了调整后的部署结构图，如图 20-33 所示，单击【应用】按钮，应用本次修改。

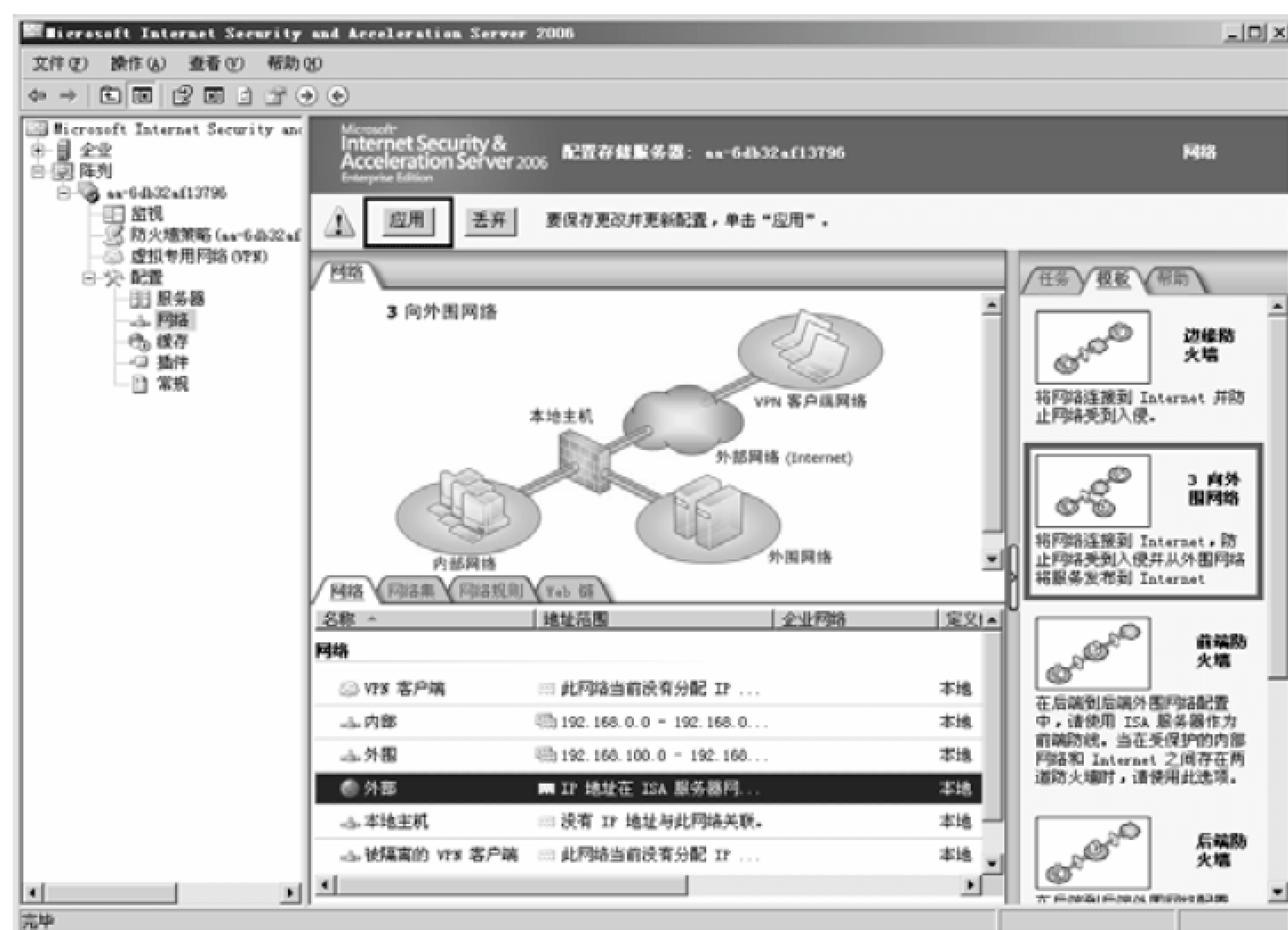


图 20-33 应用调整过的 ISA 联网部署结构

12 弹出【正在保存配置更改】对话框，如图 20-34 所示，保存完成后，单击【确定】按钮。

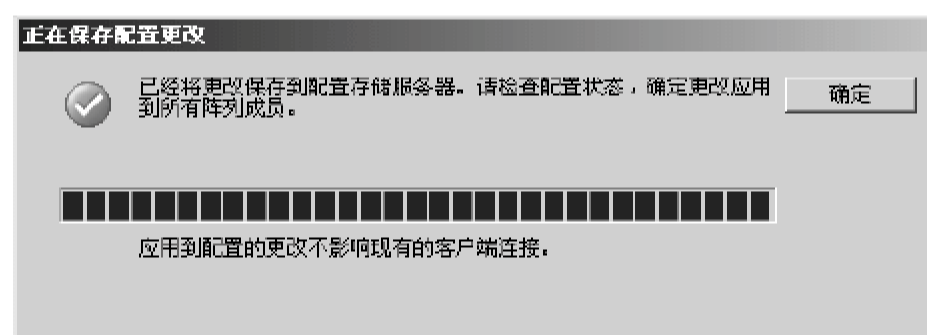


图 20-34 【正在保存配置更改】对话框

13 配置保存后并不能马上生效，ISA 服务器配置需要和存储配置服务器同步。如图 20-35 所示，在左侧选项列表中选择【监视】选项，在右侧窗格中选择【配置】选项卡，刚应用的配置尚未同步，单击右侧【任务】选项卡的【现在刷新】按钮，可以马上完成配置同步。



图 20-35 同步 ISA 服务器和存储配置服务器的配置

除了使用以上方法更换新的部署结构外，也可以通过在现有部署结构上直接增加“新网络”的方式，完成 DMZ 区的添加，具体操作步骤如下。

01 在左侧选项列表中选择【阵列】➢ aa-6db32af13796 ➢【配置】➢【网络】选项，如图 20-36 所示，选择右侧【任务】选项卡下的【创建一个新的网络】选项。



图 20-36 创建一个新网络

02 弹出【新建网络向导】对话框，如图 20-37 所示，在【网络名】文本框中输入 DMZ，单击【下一步】按钮。

03 弹出【网络类型】对话框，如图 20-38 所示，选中【外围网络】单选按钮，单击【下一步】按钮。

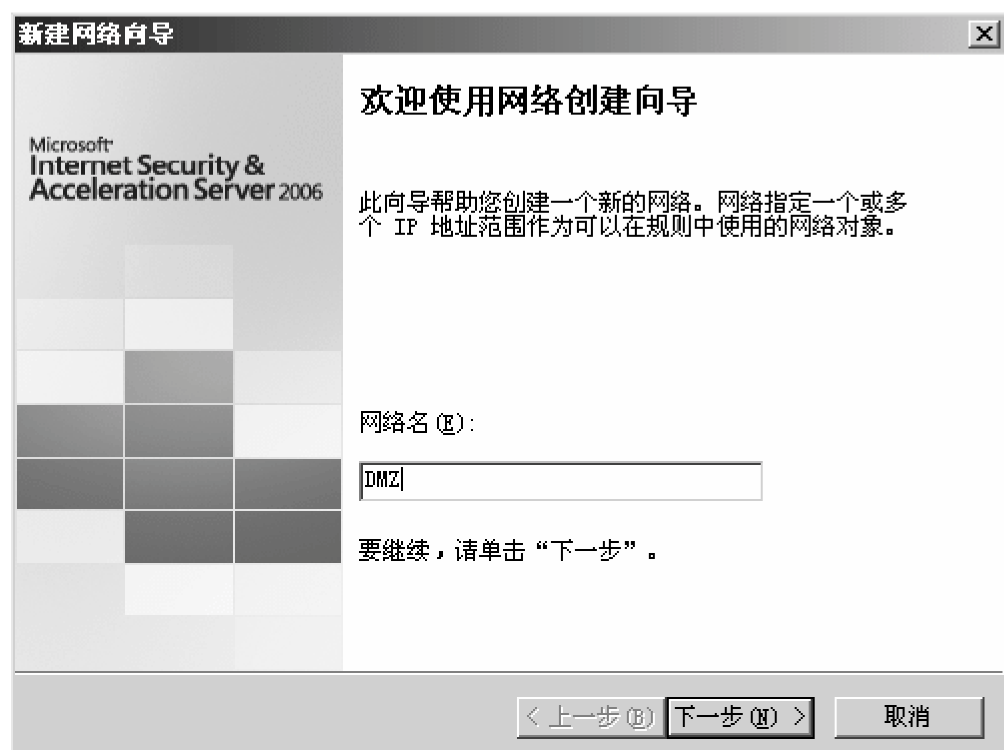


图 20-37　【新建网络向导】对话框

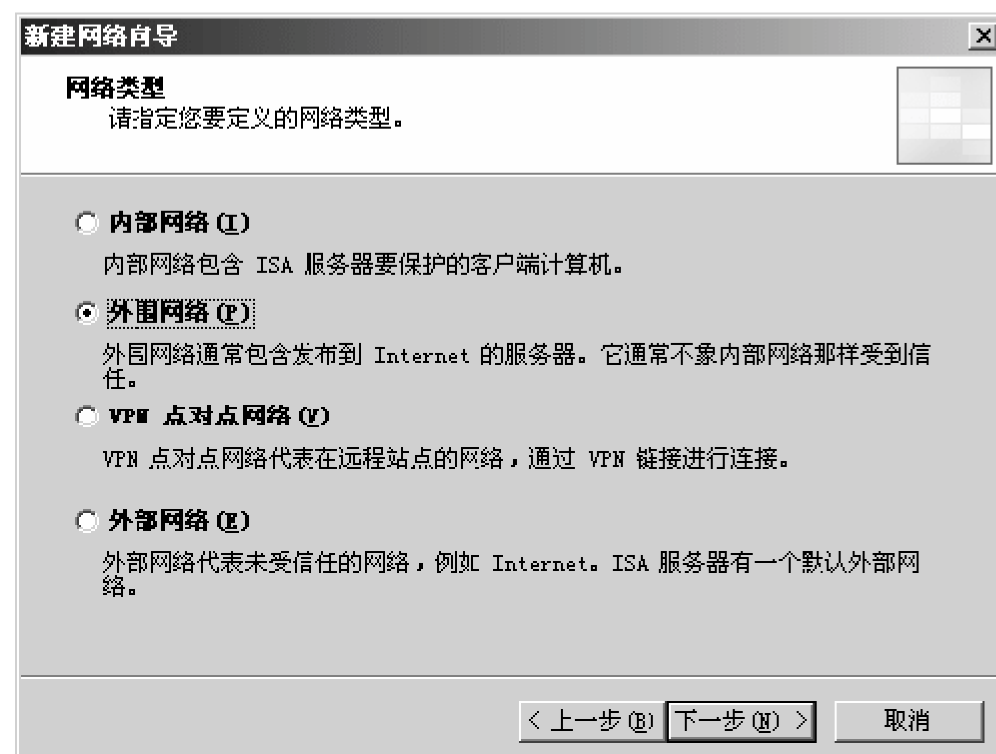


图 20-38　【网络类型】对话框

04 弹出【网络地址】对话框，如图 20-39 所示，单击【添加适配器】按钮，选择 DMZ 区连接的网卡。

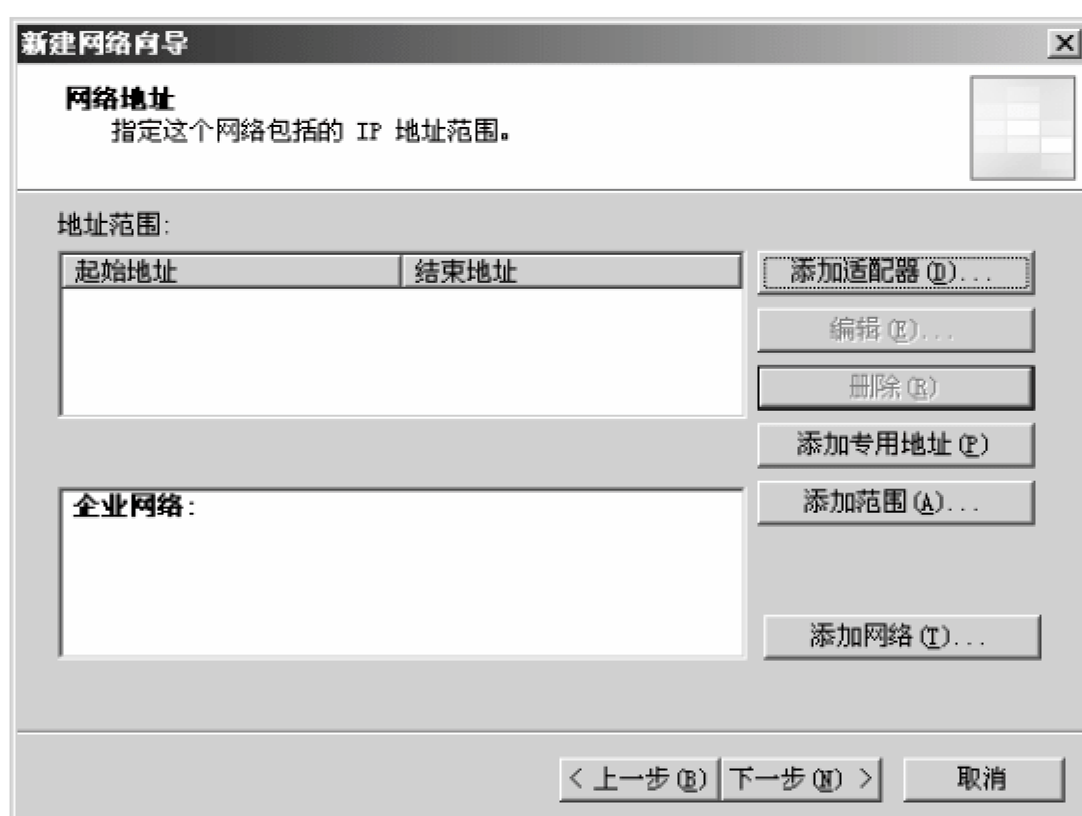


图 20-39　【网络地址】对话框



以下操作步骤与第一种操作方法类似，这里不再详细描述。

20.3　项目实战 2：利用 ISA 控制员工上网

由于业务需求，很多企业对员工的上网行为都有所约束，特别是如 QQ 空间、开心网、迅雷看看等娱乐型的网站，都会影响到员工的工作效率。因此，在架设 ISA 防火墙时，必须要准确控制员工的上网行为，具体控制方法及内容有以下几点。

20.3.1 允许员工访问互联网

由于业务需求，员工必须要有一定的网络访问权限。一般访问网络需要开启 HTTP、DNS、POP3、SMTP 等服务，具体操作步骤如下。

01 打开程序主界面，如图 20-40 所示，在左侧选项列表中选择【防火墙策略】选项，在右侧【任务】选项卡中选择【创建访问规则】选项。



图 20-40 创建访问规则

02 弹出【新建访问规则向导】对话框，如图 20-41 所示，在【访问规则名称】文本框中输入“允许员工访问外网 WEB /MAIL/DNS 服务器”，单击【下一步】按钮。

03 弹出【规则操作】对话框，如图 20-42 所示，选中【允许】单选按钮，以确保指定流量被允许通过 ISA 防火墙，单击【下一步】按钮。

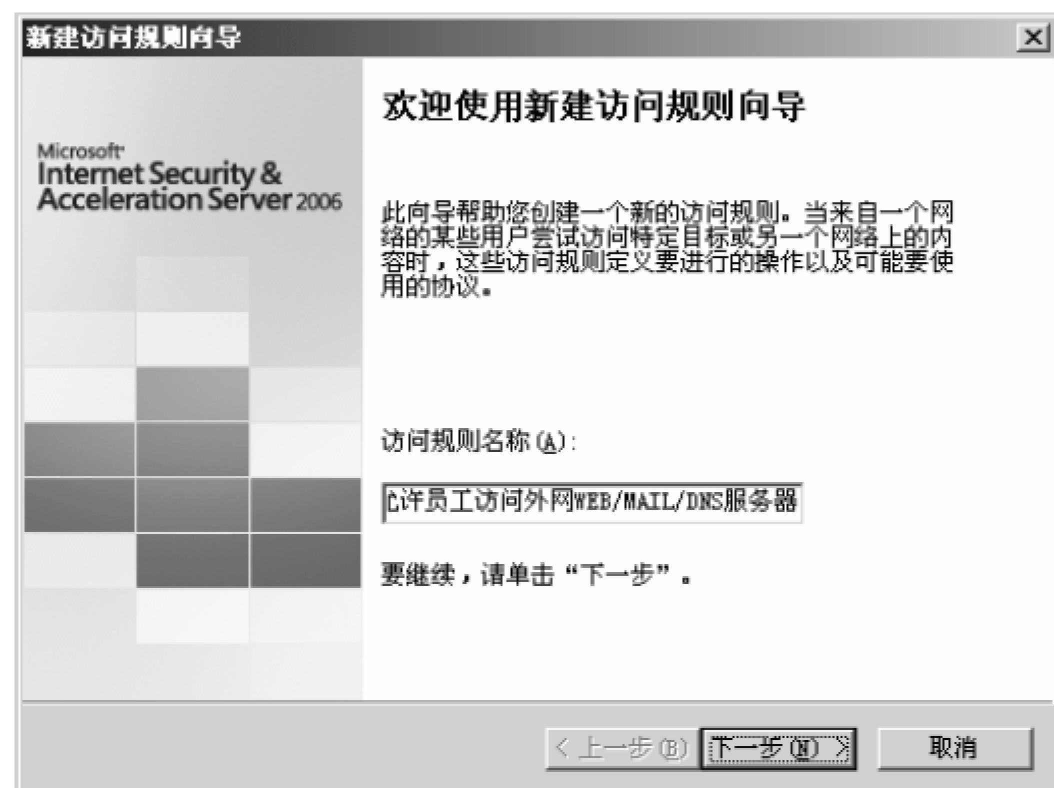


图 20-41 【新建访问规则向导】对话框

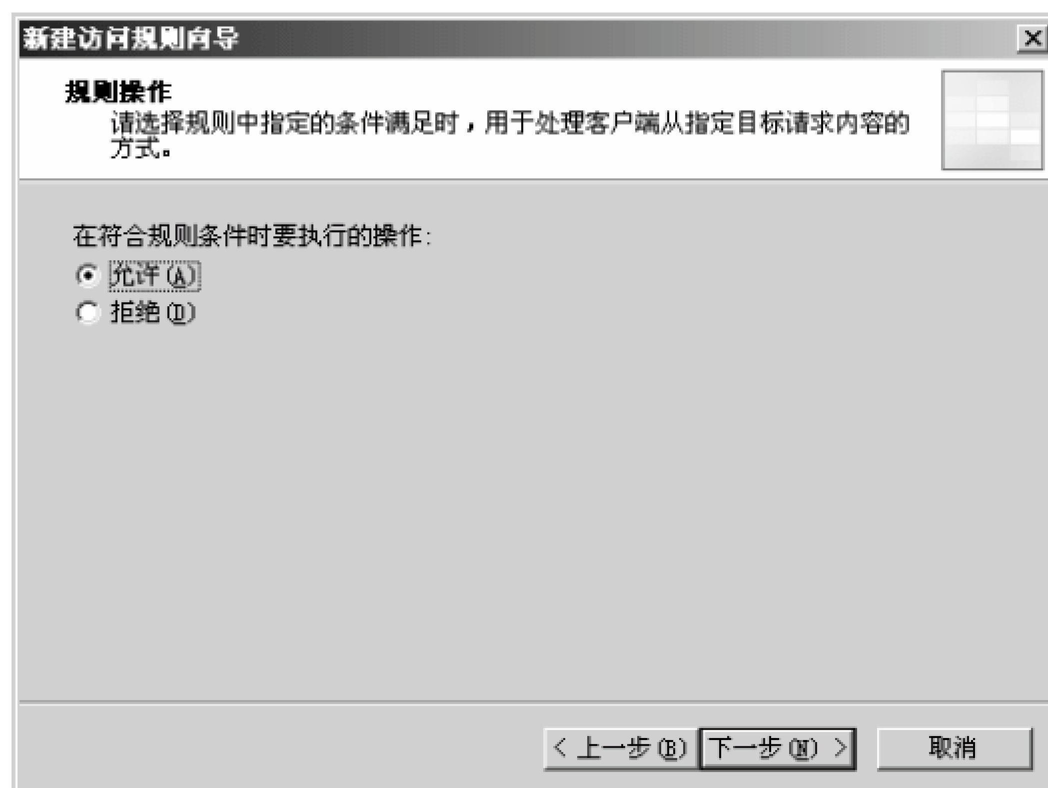


图 20-42 【规则操作】对话框

04 弹出【协议】对话框，如图 20-43 所示，在【此规则应用到】下拉列表框中选择【所选的协议】选项，单击【添加】按钮。

05 弹出【添加协议】对话框，如图 20-44 所示，在【协议】列表框中对协议进行了分类，选择 HTTP、DNS、HTTPS、POP3、SMTP 等协议，分别单击【添加】按钮。



图 20-43 【协议】对话框



图 20-44 【添加协议】对话框

06 返回【协议】对话框，如图 20-45 所示，协议添加成功。通过单击【编辑】按钮可以对指定协议进行编辑，单击【端口】按钮可以添加允许通过的端口范围，本实例不采用端口操作，单击【下一步】按钮。

07 弹出【访问规则源】对话框，如图 20-46 所示，单击【添加】按钮。



图 20-45 协议添加成功

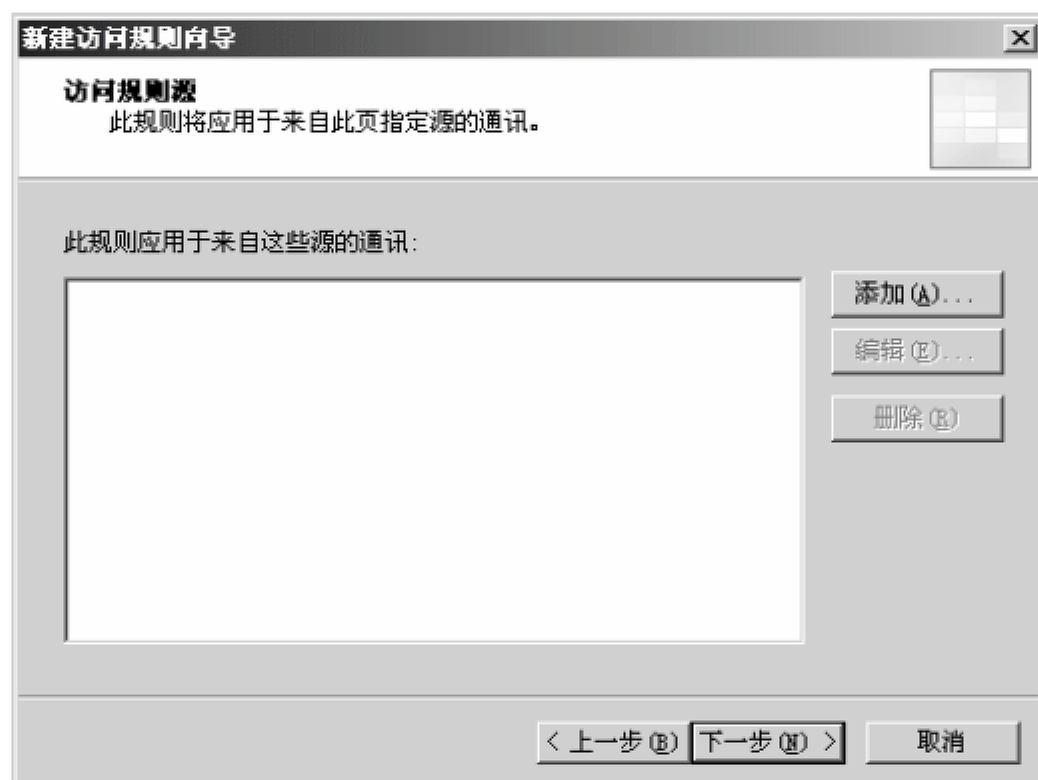


图 20-46 【访问规则源】对话框

08 弹出【添加网络实体】对话框，如图 20-47 所示，选择【网络】➢【内部】选项，单击【添加】按钮。

09 返回【访问规则源】对话框，如图 20-48 所示。“内部”代表内网，即员工所在网络，单击【下一步】按钮。



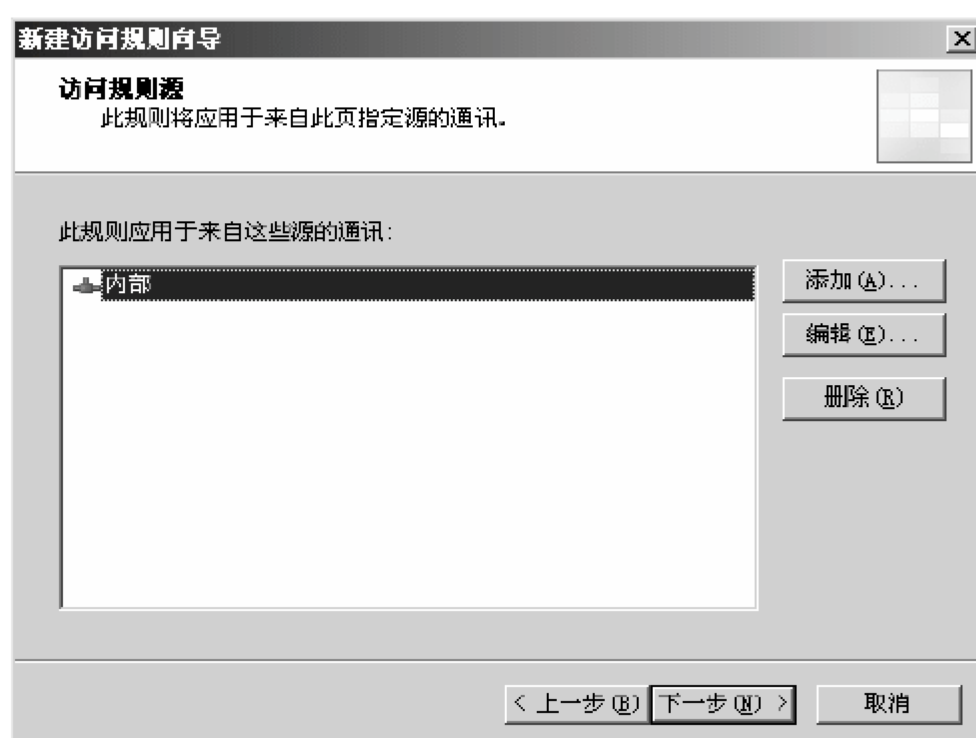
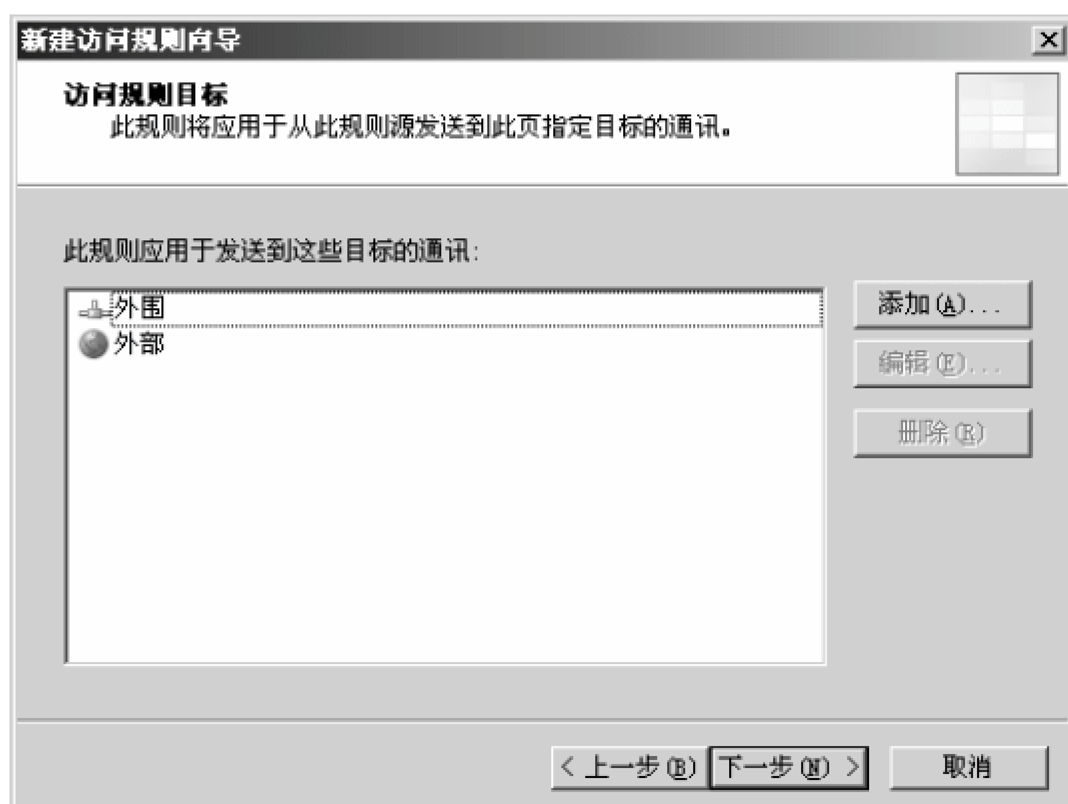


图 20-47 【添加网络实体】对话框　　　　图 20-48 网络实体添加完成

10 弹出【访问规则目标】对话框，单击【添加】按钮添加访问规则目标网络，由于员工需要有权限访问公网服务器和 DMZ 区服务器，所以要将“外围”和“外部”网络都加入访问规则目标，如图 20-49 所示，单击【下一步】按钮。

11 弹出【用户集】对话框，可以指定有权限使用该规则的用户，本实例采用【所有用户】，如图 20-50 所示，单击【下一步】按钮。



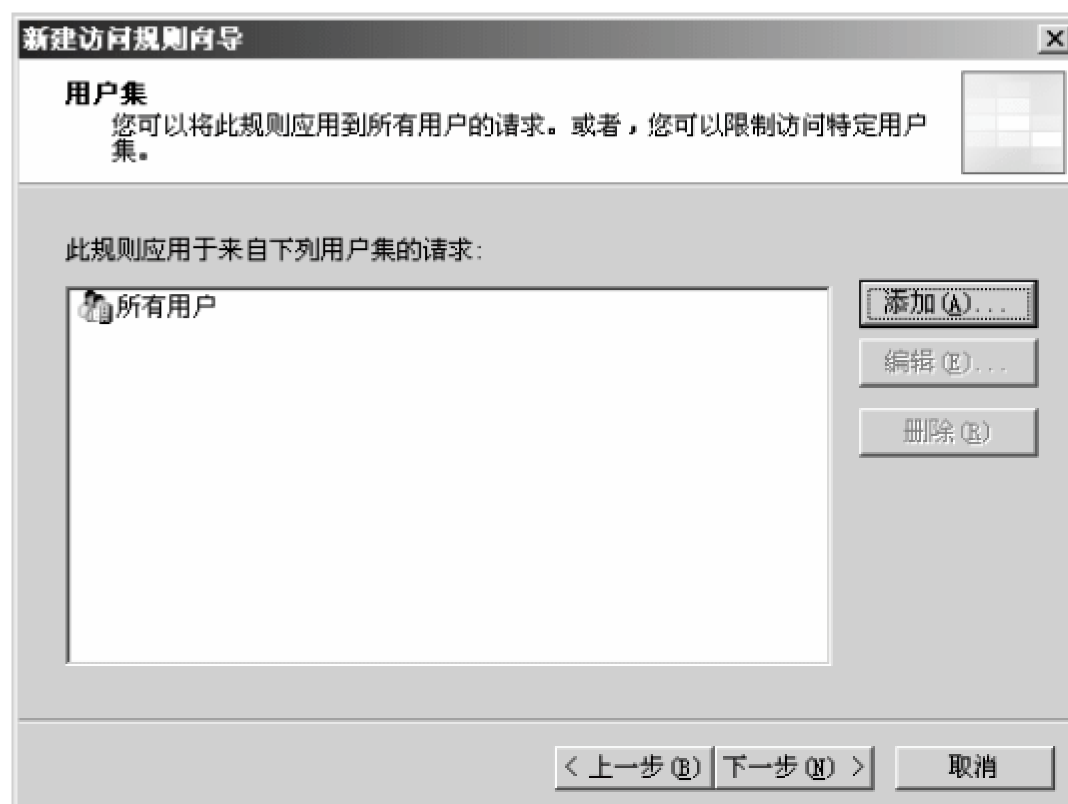


图 20-49 【访问规则目标】对话框　　　　图 20-50 【用户集】对话框

12 配置完成，在弹出的对话框中显示了允许员工访问公网的配置信息，如图 20-51 所示，单击【完成】按钮。

13 返回 ISA 防火墙主界面，如图 20-52 所示，在【防火墙策略】窗格中显示了新添加的访问规则，单击【应用】按钮，使配置生效。

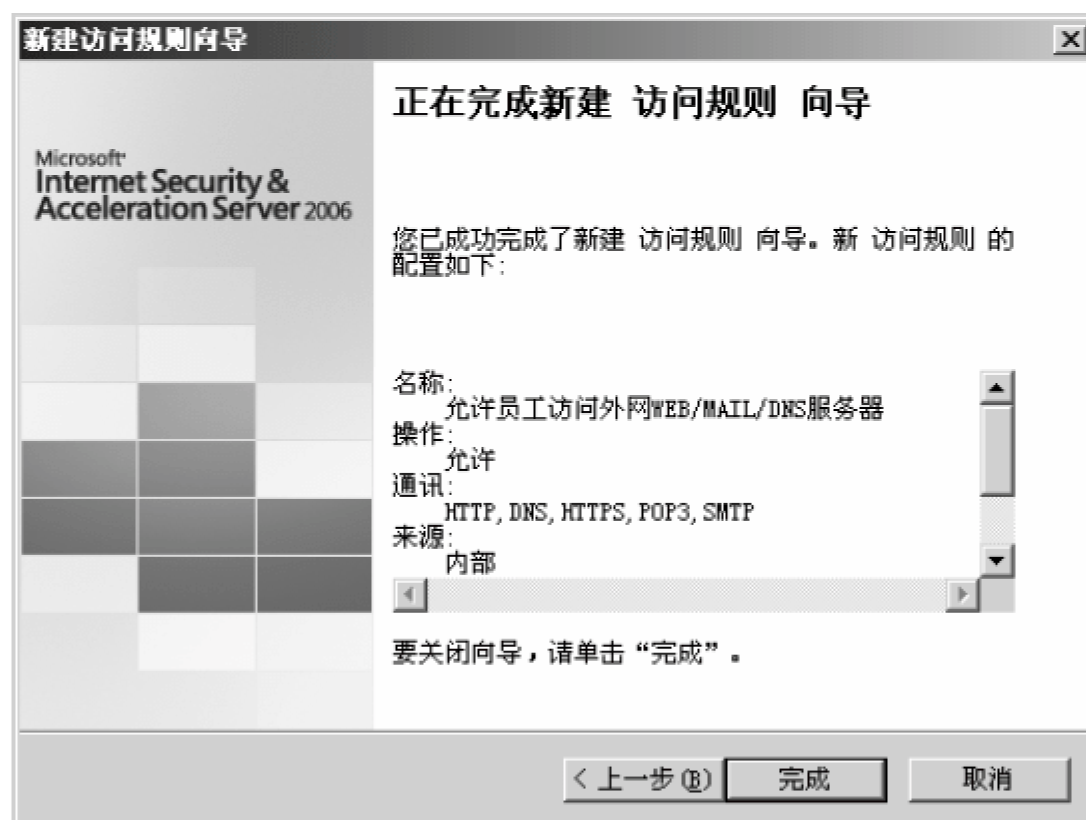


图 20-51 完成新建访问规则向导

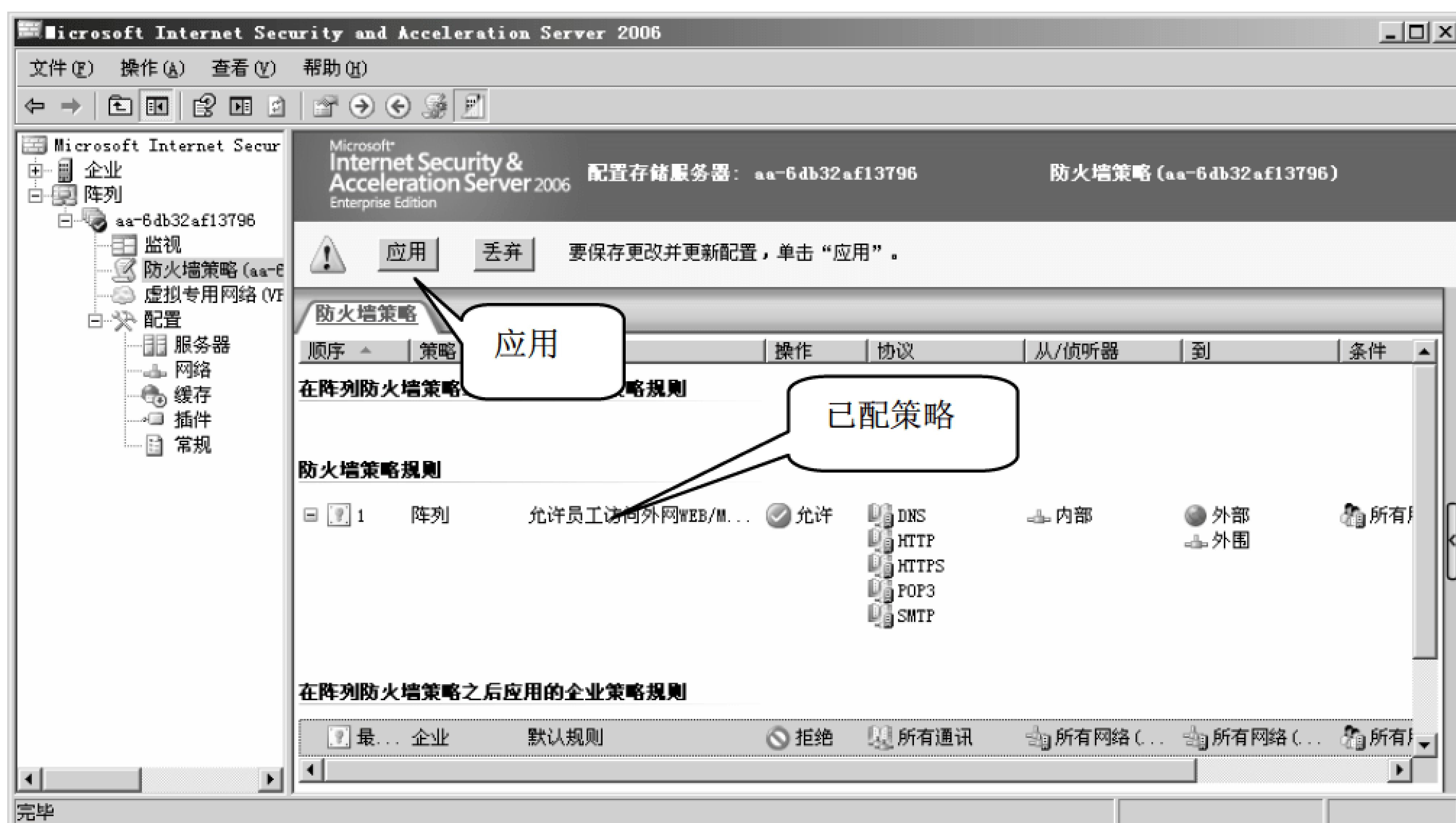


图 20-52 应用新添加访问规则

20.3.2 限制员工的上网时间

考虑到工作需要，可以限制员工上网时间段，具体操作步骤如下。

01 右击允许员工访问网络的策略，如图 20-53 所示，在弹出的快捷菜单中选择【属性】选项。

02 弹出策略属性，选择【计划】选项卡，如图 20-54 所示，默认该策略总是生效，单击【新建】按钮。

03 弹出【新建计划】对话框，如图 20-55 所示，在【名称】文本框中输入“员工上网时间”，在下侧时间区域选择不允许上网的时间段，选中【非活动】单选按钮，调整结束后，单击【确定】按钮。



图 20-53　员工访问策略属性



图 20-54　策略属性的【计划】选项卡

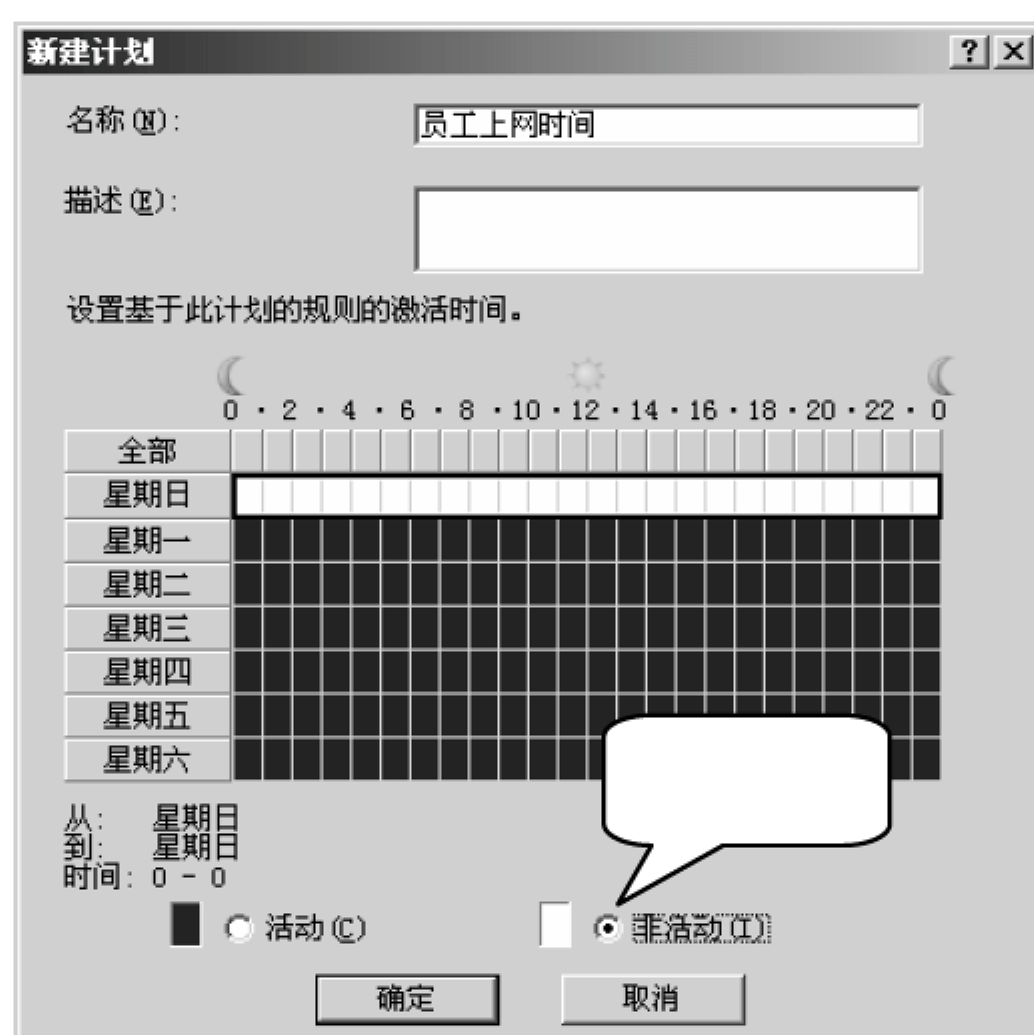


图 20-55　【新建计划】对话框

04 配置结束，返回属性对话框，如图 20-56 所示，在【计划】下拉列表框中选择“员工上网时间”，单击【确定】按钮。

05 返回程序主界面，如图 20-57 所示，单击【应用】按钮，使配置生效。

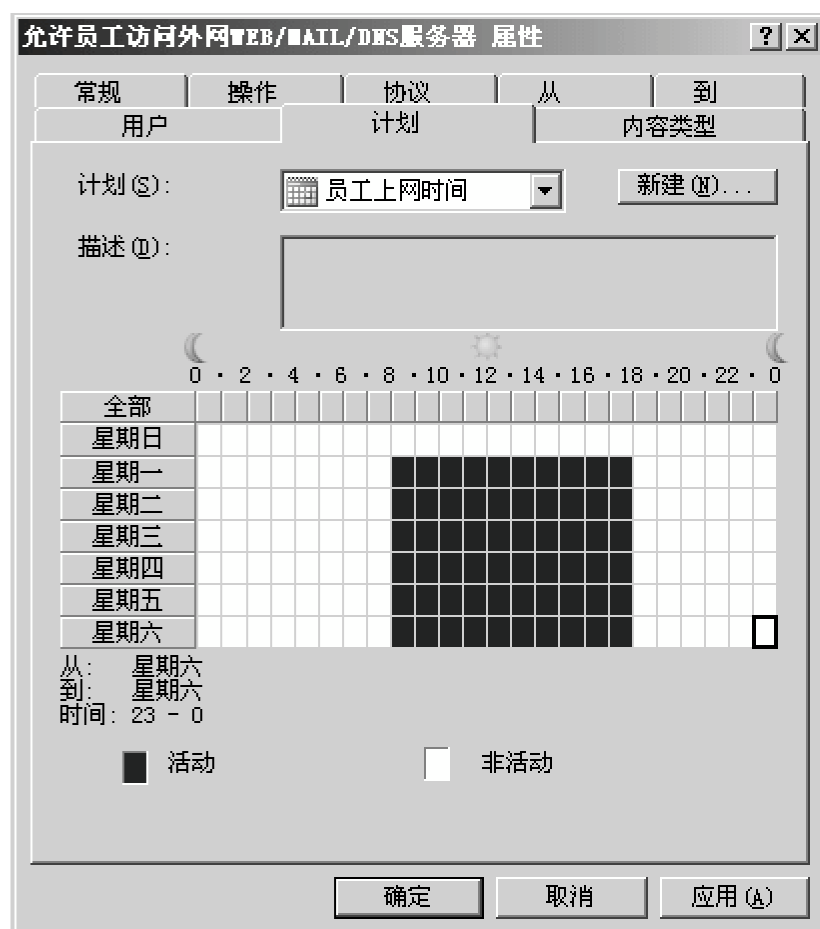


图 20-56　选择新建计划

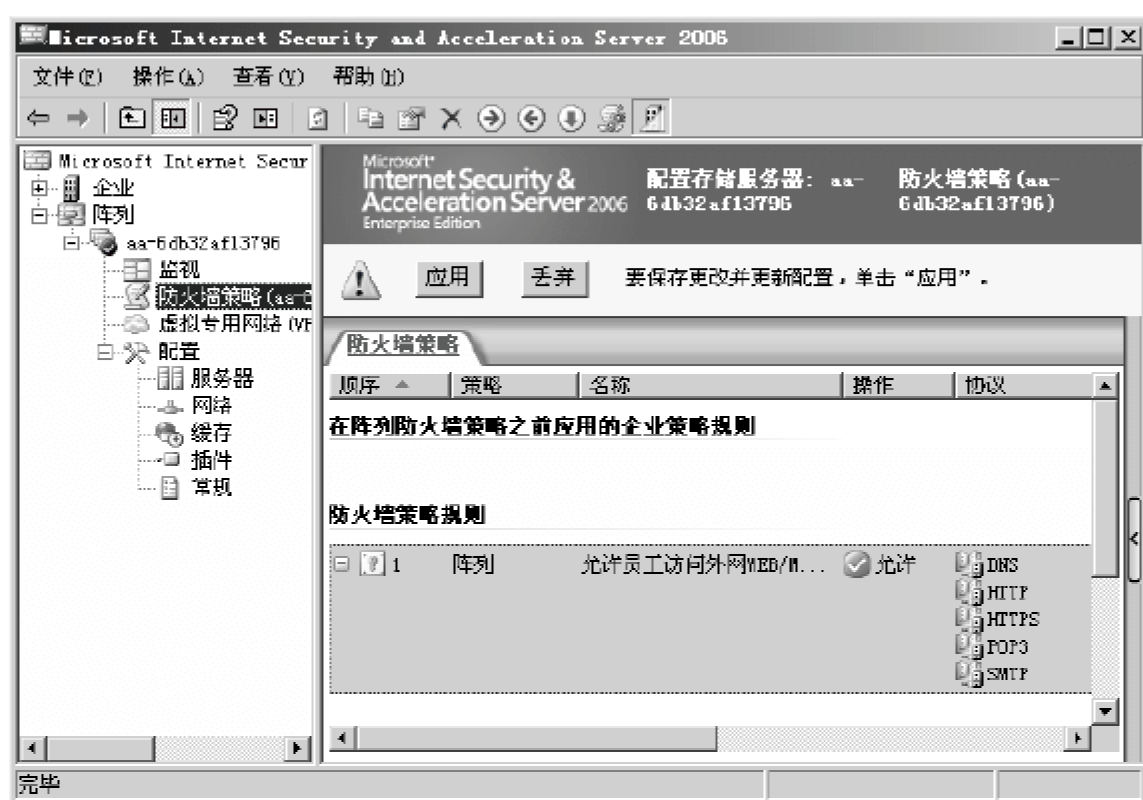


图 20-57　应用策略属性修改

20.3.3　限制员工访问特殊域名网站

信息产业飞速发展，各类娱乐网站层出不穷，如 QQ 空间、开心网、迅雷看看等。很多员工沉迷于这些网站，如前几年的“偷菜”热，“偷菜”几乎成了人们生活、工作中的一部分。这让很多领导烦恼不已。对此，ISA 防火墙可以做出针对性的限制，具体操作步骤如下。

01 打开【新建访问规则向导】对话框，如图 20-58 所示，在【访问规则名称】文本框中输入“不允许员工访问 QQ 空间等娱乐网站”，单击【下一步】按钮。

02 弹出【规则操作】对话框，如图 20-59 所示，选中【拒绝】单选按钮，单击【下一步】按钮。

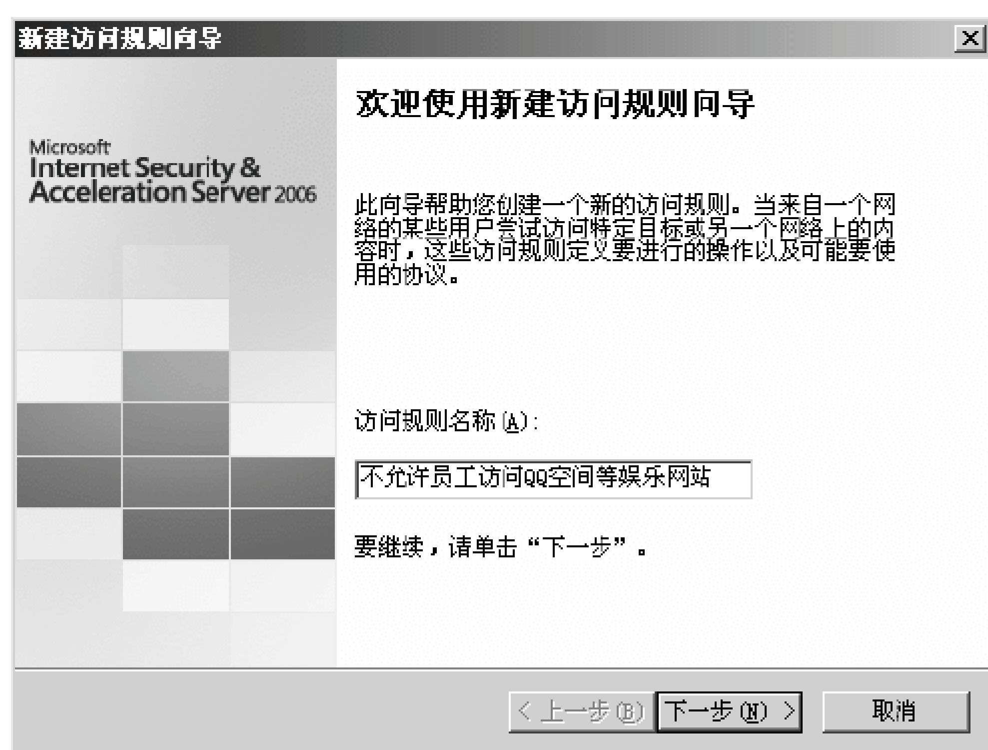


图 20-58　【新建访问规则向导】对话框

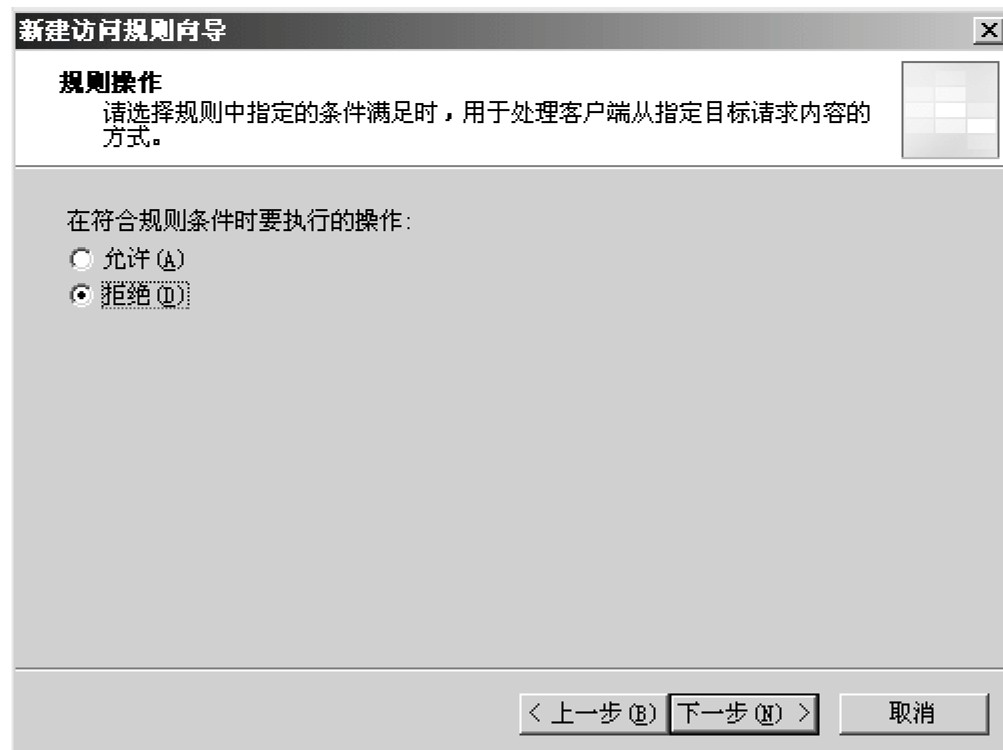


图 20-59　【规则操作】对话框

03 弹出【协议】对话框，通过【添加】按钮，将 DNS\HTTP\HTTPS 等协议加入列表，如图 20-60 所示，单击【下一步】按钮。

04 弹出【访问规则源】对话框，如图 20-61 所示，将【内部】网络加入列表框中，单击【下一步】按钮。

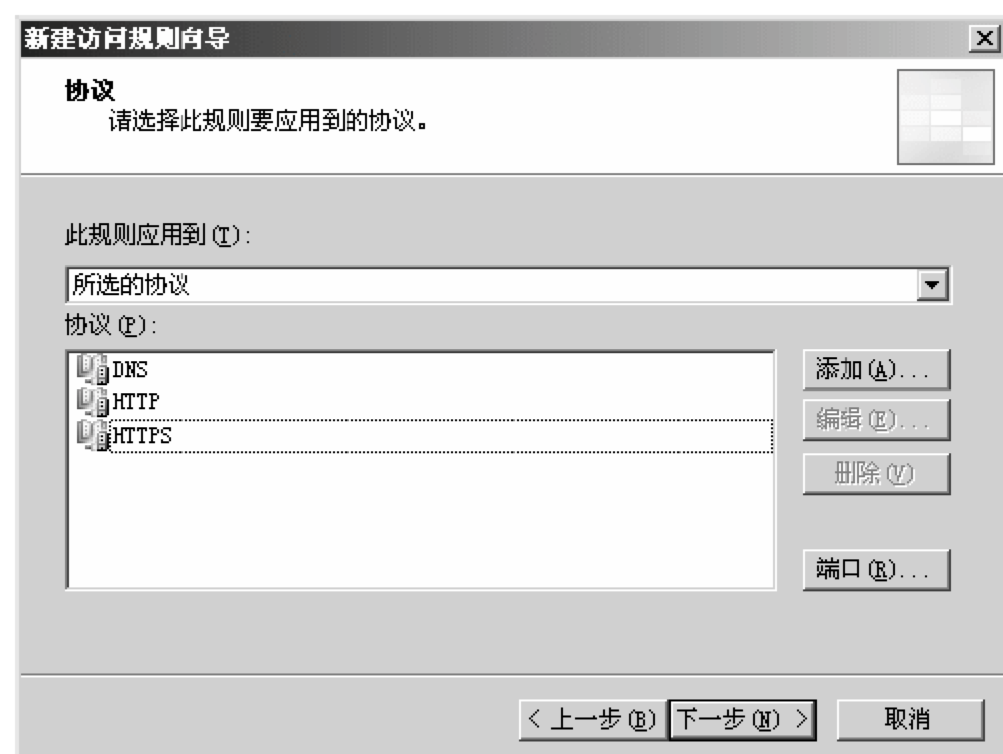


图 20-60 【协议】对话框

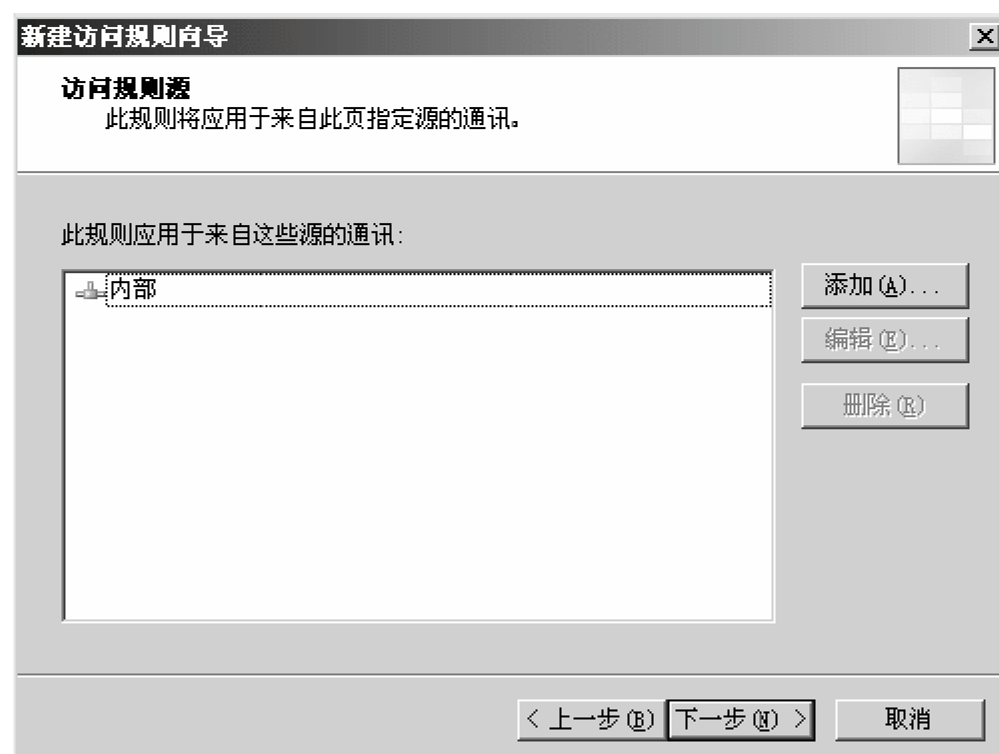


图 20-61 【访问规则源】对话框

05 弹出【访问规则目标】对话框，单击【添加】按钮，弹出【添加网络实体】对话框，在【网络实体】列表框中选择【新建】➢【URL 集】命令，如图 20-62 所示。

06 弹出【新建 URL 集规则元素】对话框，如图 20-63 所示，在【名称】文本框中输入“员工不可访问网站”，单击【添加】按钮可在【此集包含的 URL】列表框中添加具有匹配特征的网址。

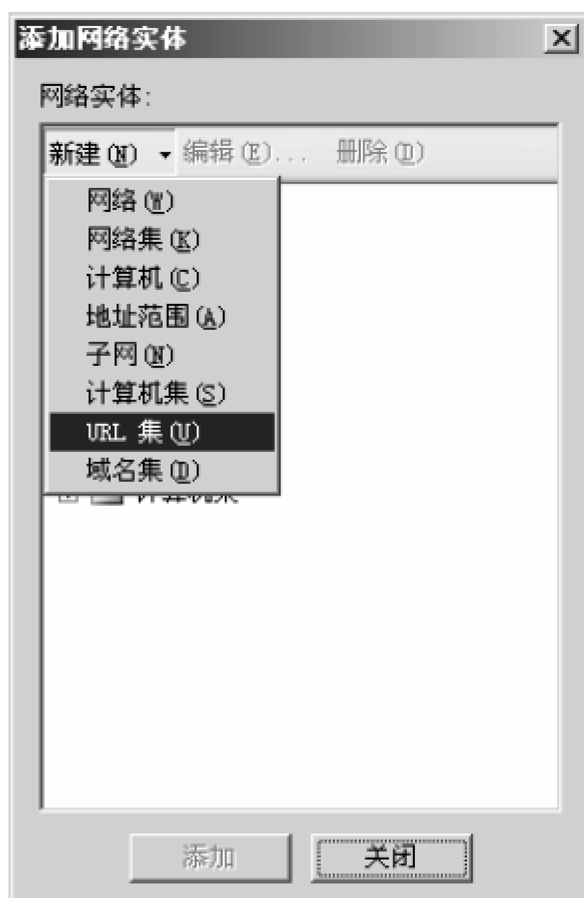


图 20-62 【访问规则目标】对话框

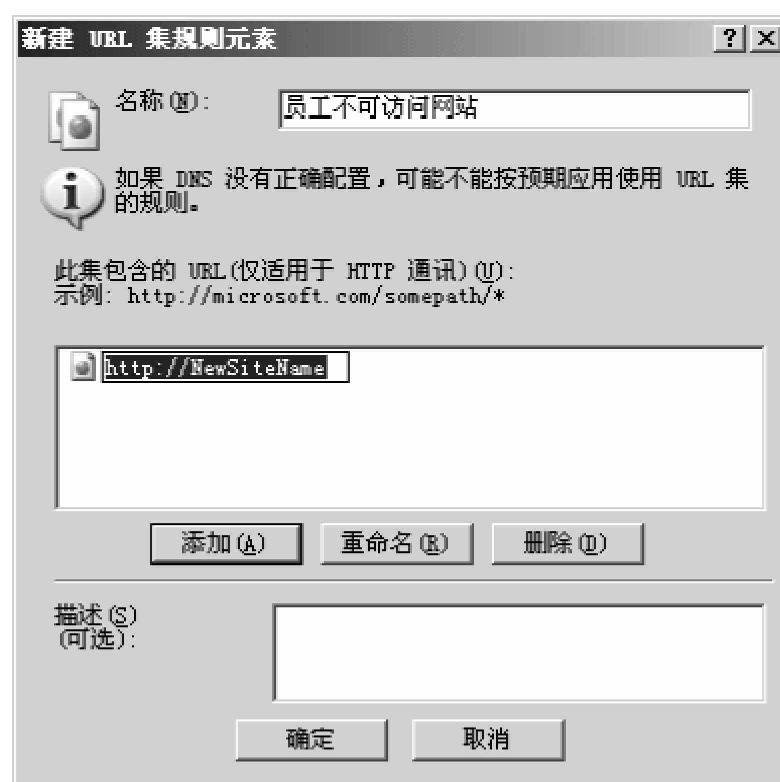


图 20-63 【新建 URL 集规则元素】对话框

07 如图 20-64 所示，员工不可访问网址添加完成，其中“*”号代表匹配任意字符串，单击【确定】按钮。

08 返回【访问规则目标】对话框，如图 20-65 所示，不可访问目标网站添加成功，单击【下一步】按钮。

09 弹出【用户集】对话框，如图 20-66 所示，默认将该规则应用到所有用户的请求，单击【下一步】按钮。

10 配置完成，在弹出的对话框中显示了配置信息摘要，如图 20-67 所示，单击【完成】按钮，并在程序主界面应用该配置。

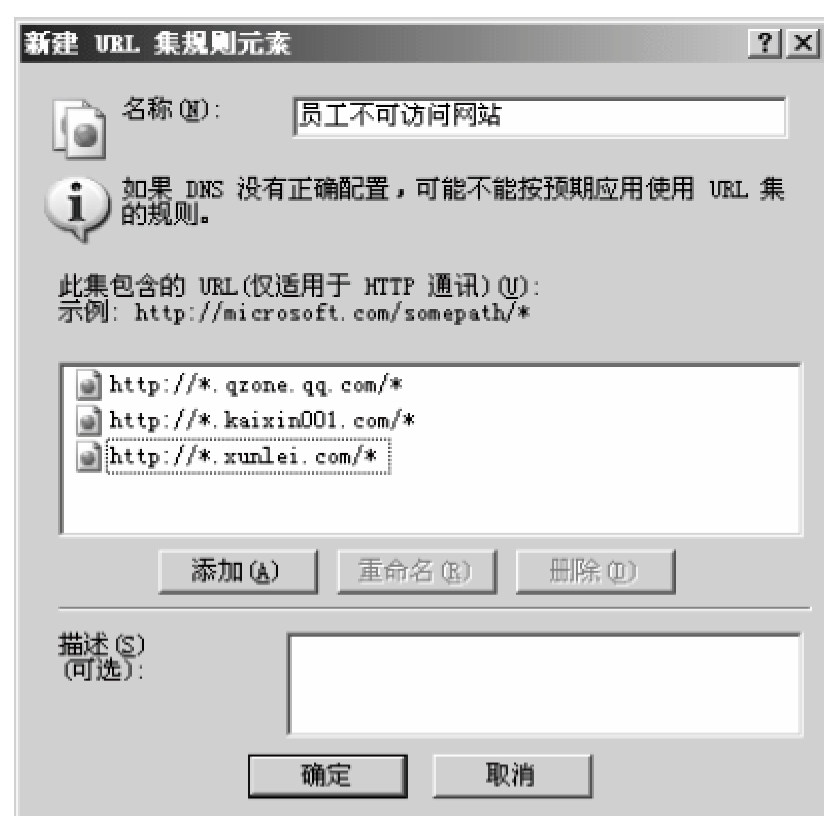


图 20-64　员工不可访问网址添加完成

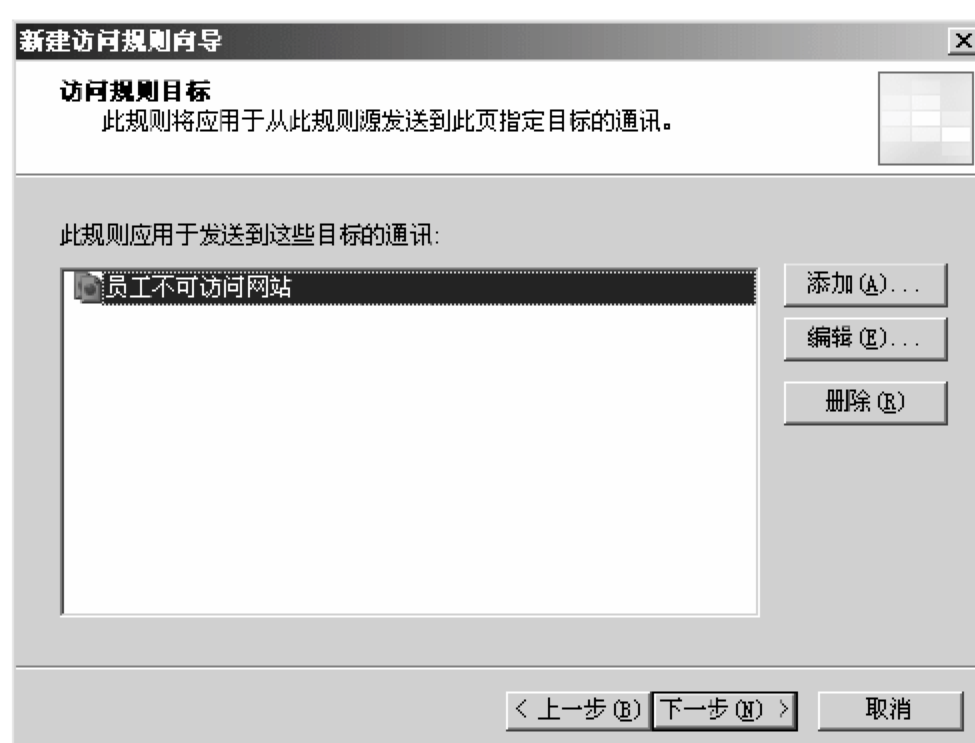


图 20-65　不可访问网站添加成功

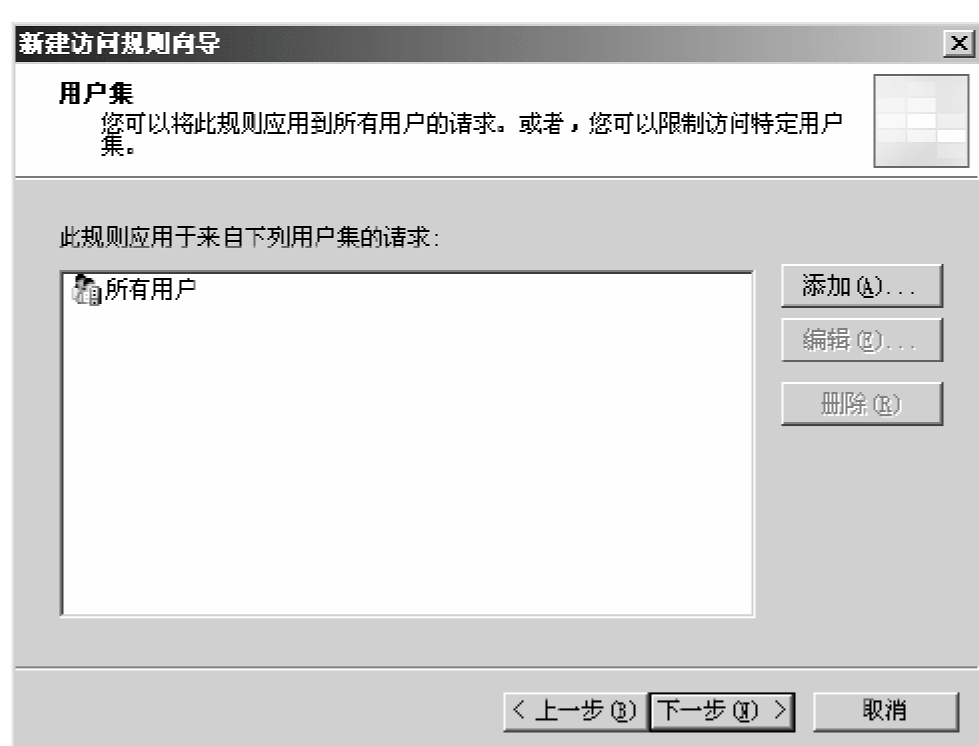


图 20-66　【用户集】对话框

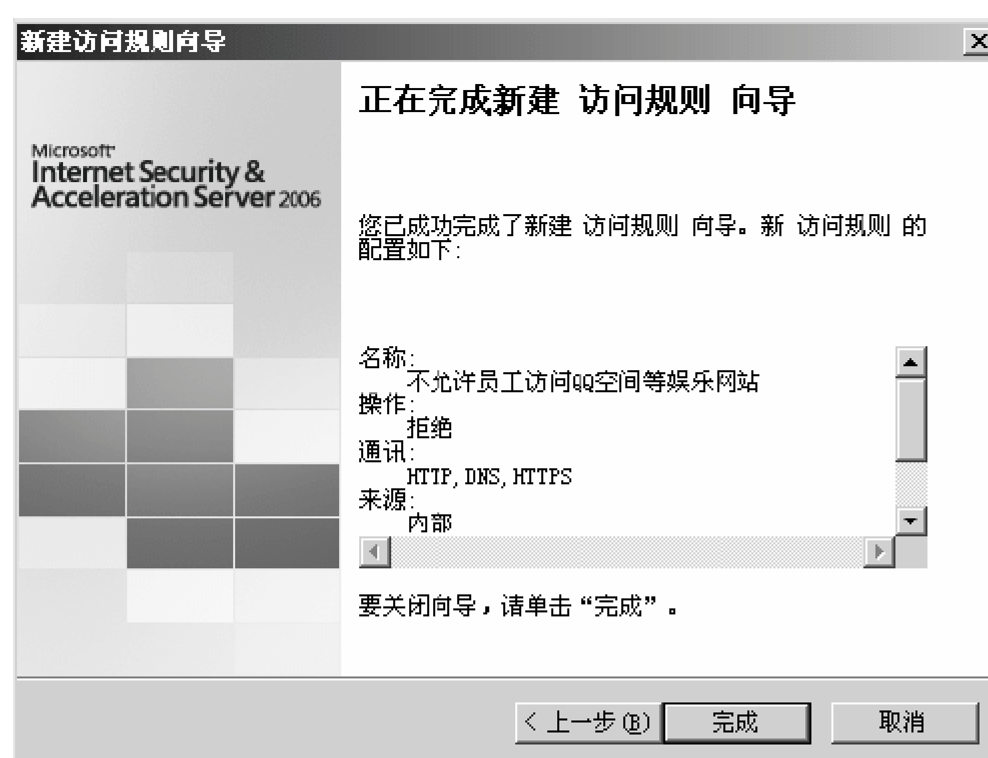


图 20-67　新建访问规则向导完成

20.3.4　限制员工使用迅雷等下载工具

企业的网络带宽资源一般都很有限，特别是中小企业。有限的资源如果被恶意占用，会严重影响公司业务的实现。其中影响较大的就是在线视频、网络下载。在线视频可以通过 20.3.2 节进行域名限制，下面主要介绍网络下载的限制方法。

1. 封锁 HTTP 下载

很多浏览器自带下载功能，通常情况下这部分网络下载流量会被网络管理员忽略，但是如果放任不管的话，依然会造成很大比例的网络资源浪费。

限制 HTTP 下载的具体操作步骤如下。

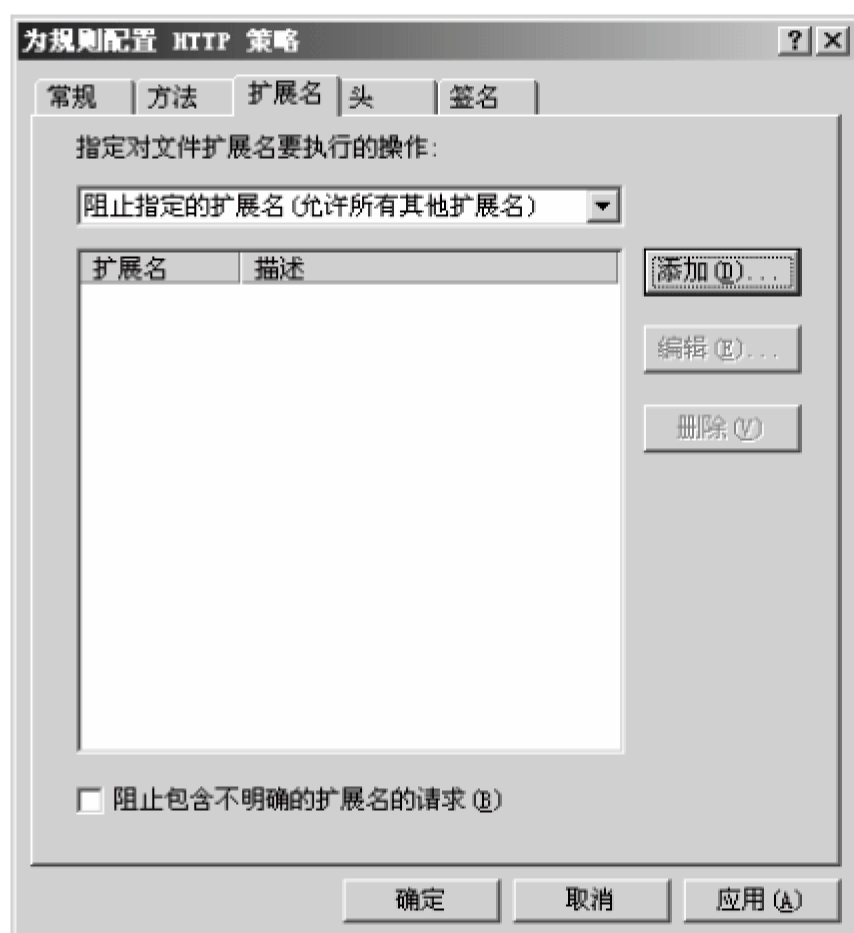
01 右击允许员工访问互联网的防火墙策略，在弹出的快捷菜单中选择【配置 HTTP】命令，如图 20-68 所示。



图 20-68　允许员工访问互联网策略的快捷菜单

02 弹出【为规则配置 HTTP 策略】对话框，如图 20-69 所示，选择【扩展名】选项卡，在【指定对文件扩展名要执行的操作】下拉列表框中选择【阻止指定的扩展名(允许所有其他扩展名)】选项，单击【添加】按钮。

03 弹出【扩展名】对话框，如图 20-70 所示，在【扩展名】文本框中输入可能被下载的文件后缀，一般视频媒体文件被设定为禁止下载内容，单击【确定】按钮，完成添加。



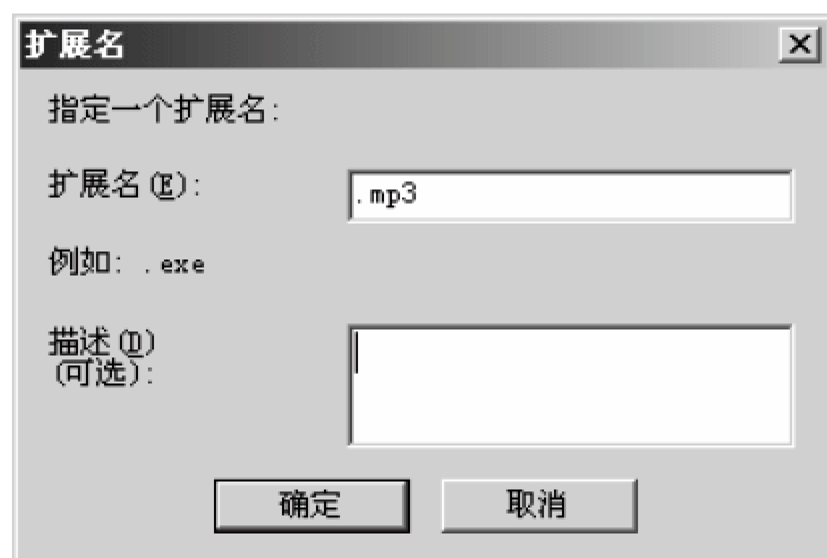


图 20-69　【为规则配置 HTTP 策略】对话框　　图 20-70　【扩展名】对话框

04 按照上述步骤添加被限制下载的所有文件类型，添加结果如图 20-71 所示，选中【阻止包含不明确的扩展名的请求】复选框，单击【确定】按钮。



图 20-71 添加被限制下载的文件类型

05 返回程序主界面，如图 20-72 所示，单击【应用】按钮使配置生效。

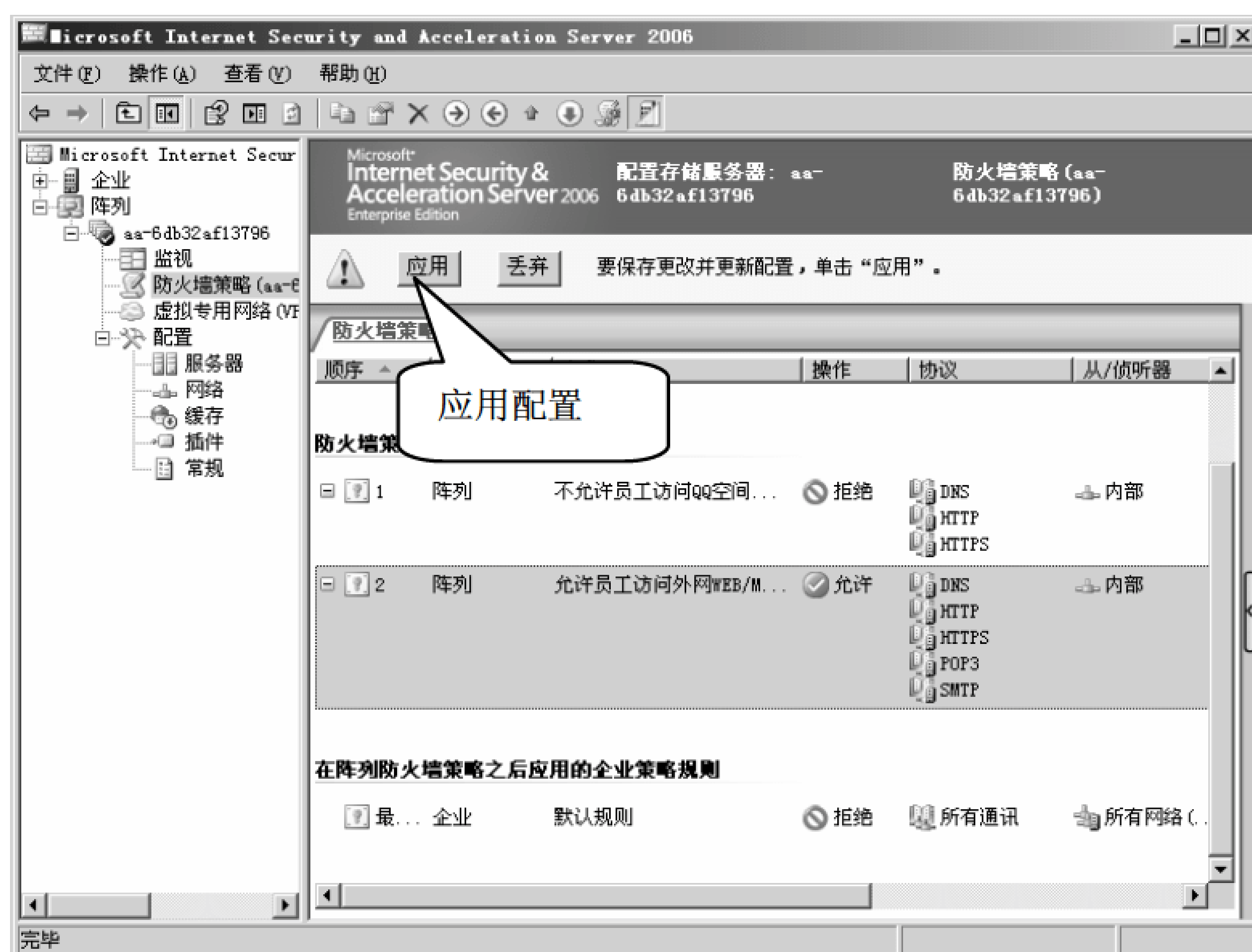


图 20-72 应用设定的网络下载限制

2. 封锁迅雷和 BT

一般封锁迅雷比较难操作，可以使用“封锁 HTTP 下载”的方式。如果想彻底封锁迅雷可以通过网络搜索所有迅雷的服务器 IP 地址，将这些地址封掉就可以了，但是迅雷的服务器 IP 地址比较多，操作起来会有些麻烦。

BT 流量的封锁也可以使用“封锁 HTTP 下载”的方式。同时还可以使用签名的方式封锁 BT。当 BT 客户端下载时，在 HTTP 请求的数据包中，包含了带有 BT 特征的头(User-Agent): BitTorrent。详细操作步骤如下。

01 右击允许员工访问互联网的防火墙策略，在快捷菜单中选择【配置 HTTP】命令，弹出【为规则配置 HTTP 策略】对话框。如图 20-73 所示，选择【签名】选项卡，单击【添加】按钮。

02 弹出【签名】对话框，如图 20-74 所示，在【名称】文本框中输入本条签名名称“BT 流量”，在【查找范围】下拉列表框中选择【请求头】选项，在【HTTP 头】文本框中输入 User-Agent，在【签名】文本框中输入 BitTorrent，单击【确定】按钮。



图 20-73 【签名】选项卡



图 20-74 【签名】对话框

03 如图 20-75 所示，返回程序主界面，单击【应用】按钮使配置生效。

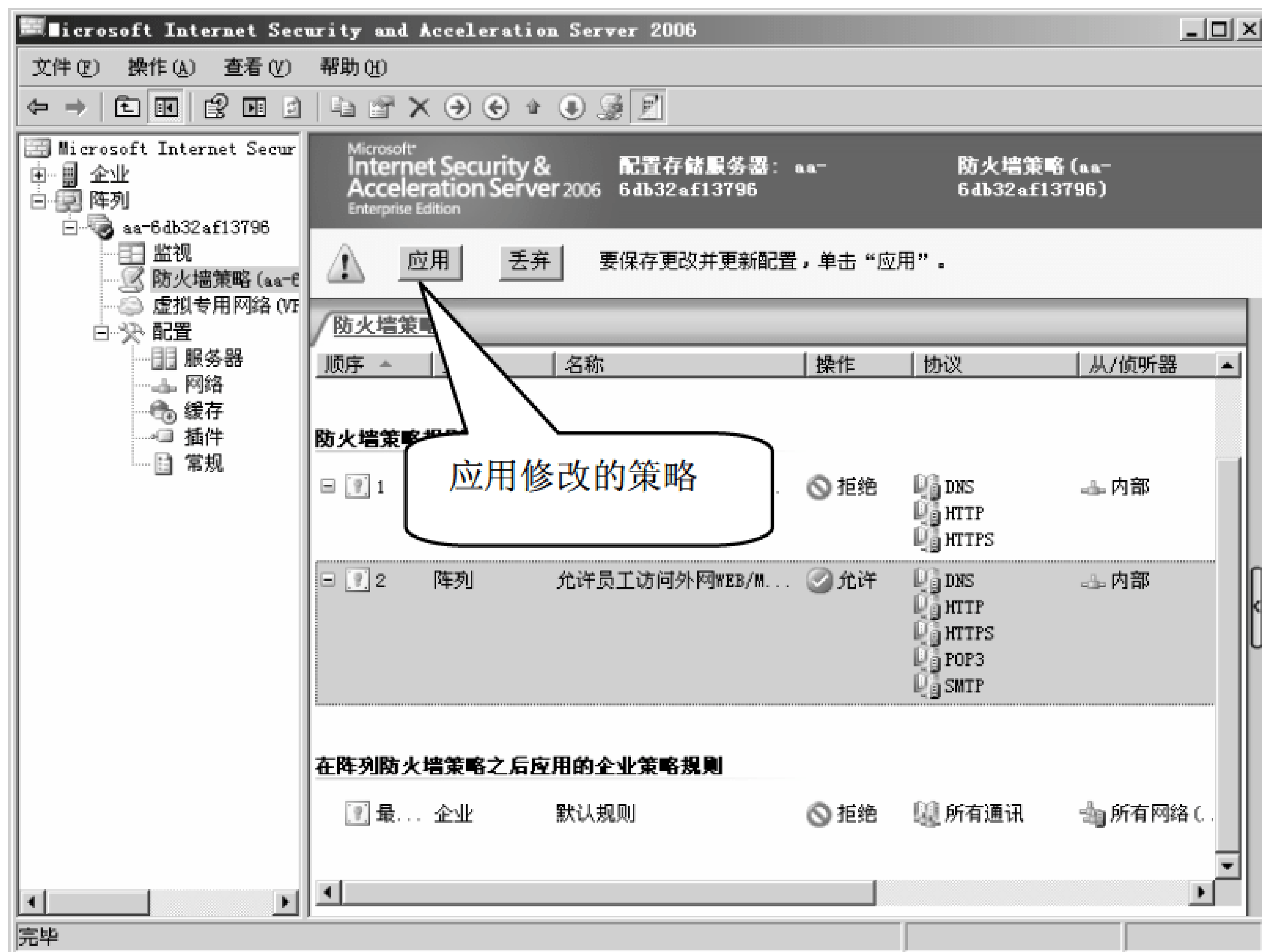


图 20-75 应用修改的策略

20.4　项目实战 3：利用 ISA 发布企业内网服务器

在 DMZ 区放置了企业对外发布服务器，主要有 Web 服务器、DNS 服务器、E-mail 服务器等。下面详细介绍这些服务器的发布。

20.4.1　ISA 防火墙安全发布 Web 服务器

Web 服务器是企业最重要的对外发布服务器之一，几乎大部分企业都会用到。

单一 Web 服务器的发布操作步骤如下。

01 在左侧列表中选择【防火墙策略】选项，在右侧窗格选择【任务】选项卡，选择【发布网站】选项，如图 20-76 所示。



图 20-76　发布网站

02 弹出【新建 Web 发布规则向导】对话框，如图 20-77 所示，在【Web 发布规则名称】文本框中输入“DMZ 区对外发布 WEB 服务器”，单击【下一步】按钮。

03 弹出【请选择规则操作】对话框，如图 20-78 所示，选中【允许】单选按钮，单击【下一步】按钮。

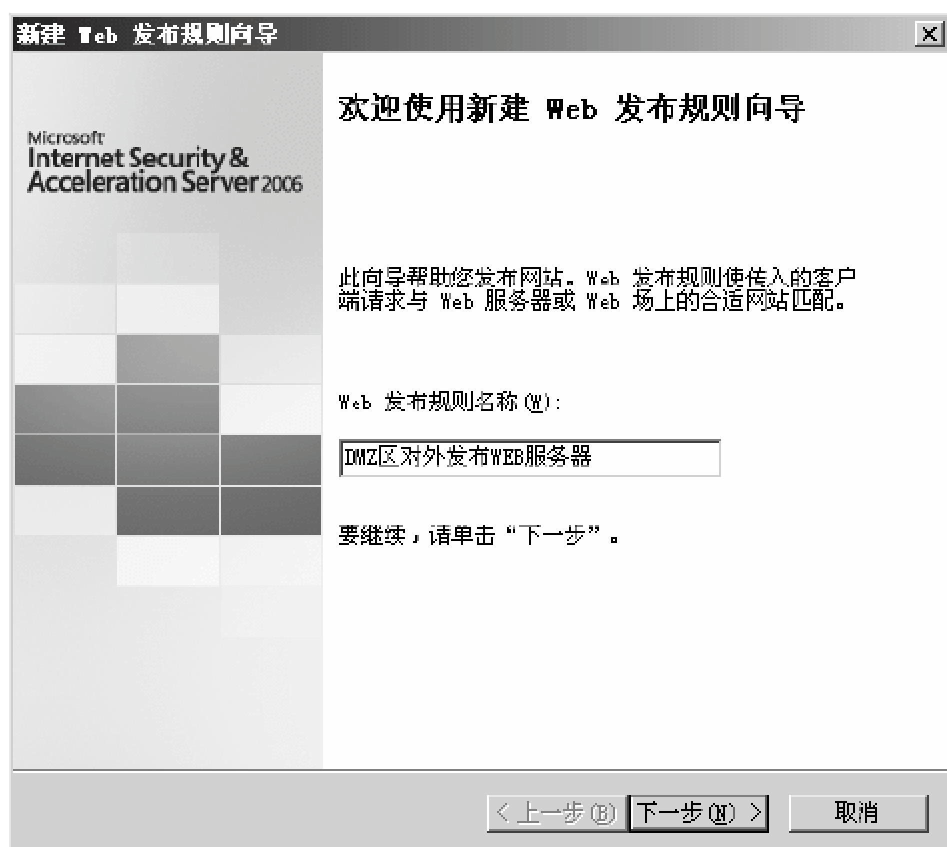


图 20-77 【新建 Web 发布规则向导】对话框

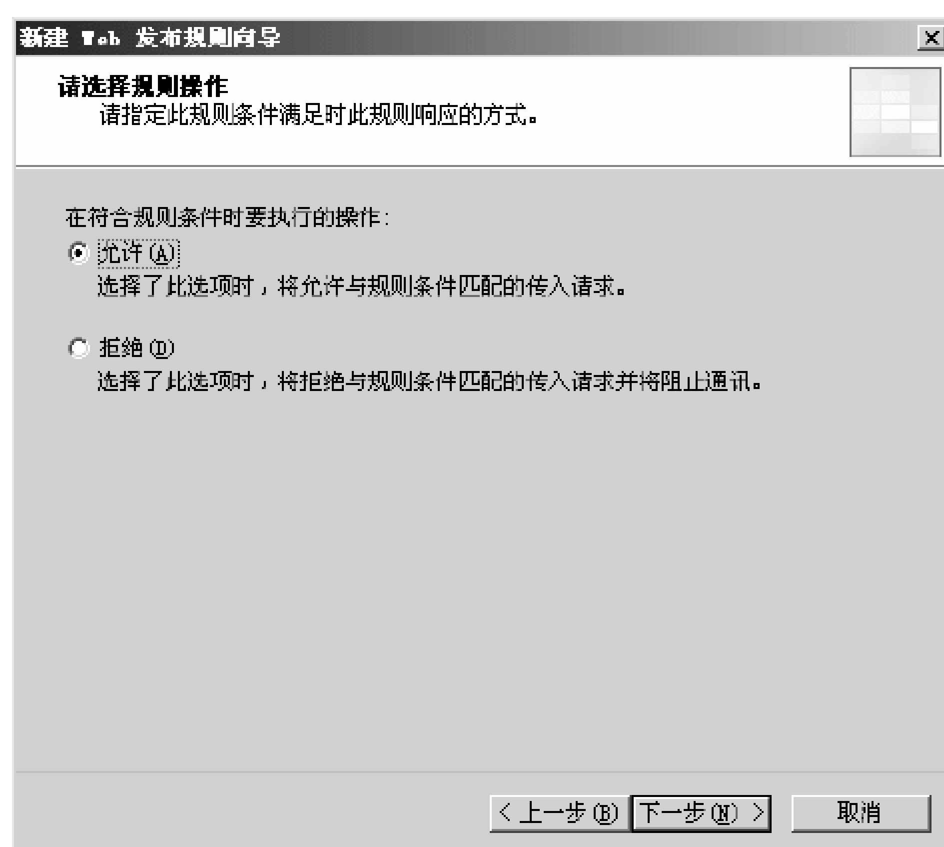


图 20-78 【请选择规则操作】对话框

04 弹出【发布类型】对话框，如图 20-79 所示，选中【发布单个网站或负载平衡器】单选按钮，单击【下一步】按钮。

05 弹出【服务器连接安全】对话框，如图 20-80 所示，选中【使用不安全的连接发布的 Web 服务器或服务器场】单选按钮。

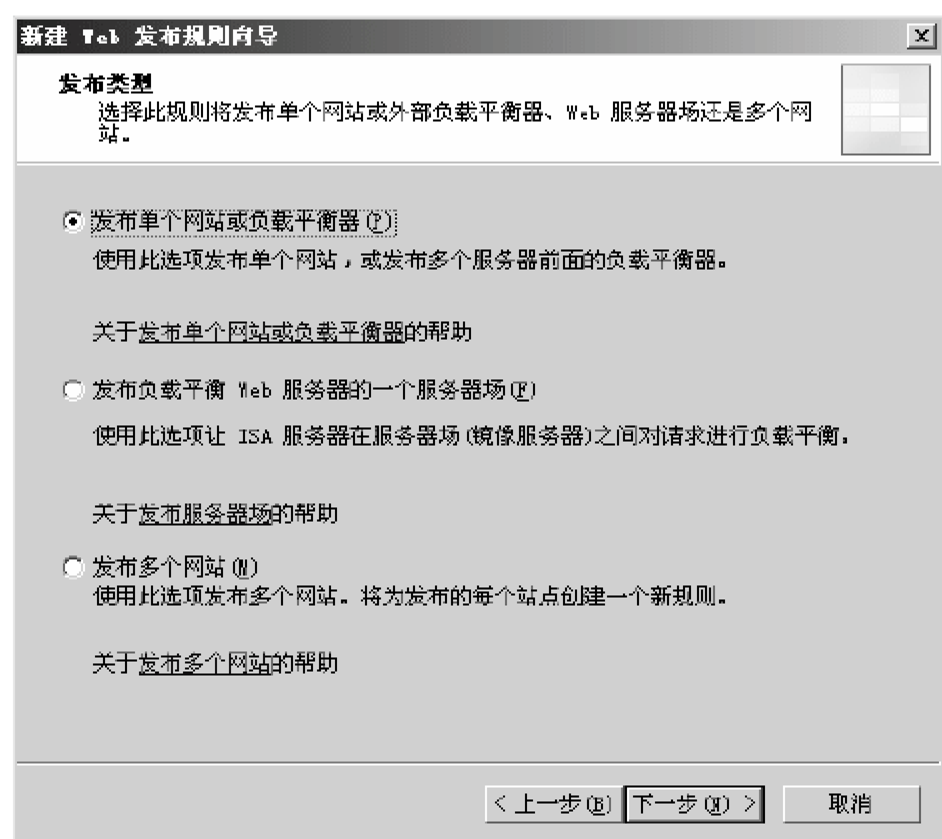


图 20-79 【发布类型】对话框

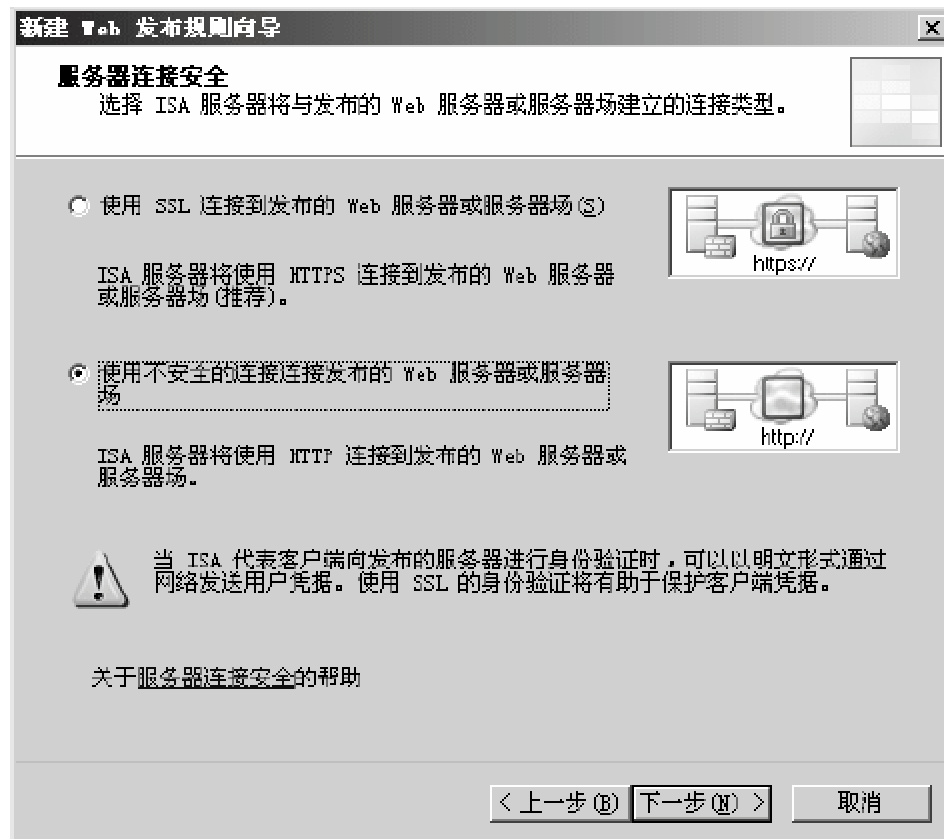


图 20-80 【服务器连接安全】对话框



提 示

如果使用 SSL 连接发布服务器，必须要有认证系统，否则网站发布会失败，本实例不做 SSL 连接。

06 弹出【内部发布详细信息】对话框，如图 20-81 所示，在【内部站点名称】文本框中输入网站在内网使用的域名，本实例采用“www.Web .com”，为了内网服务器可以被访问到，在【计算机名称或 IP 地址】文本框中输入 DMZ 区 Web 服务器的 IP 地址“192.168.100.100”，单击【下一步】按钮。

07 在弹出的对话框中选择默认配置，如图 20-82 所示，单击【下一步】按钮。

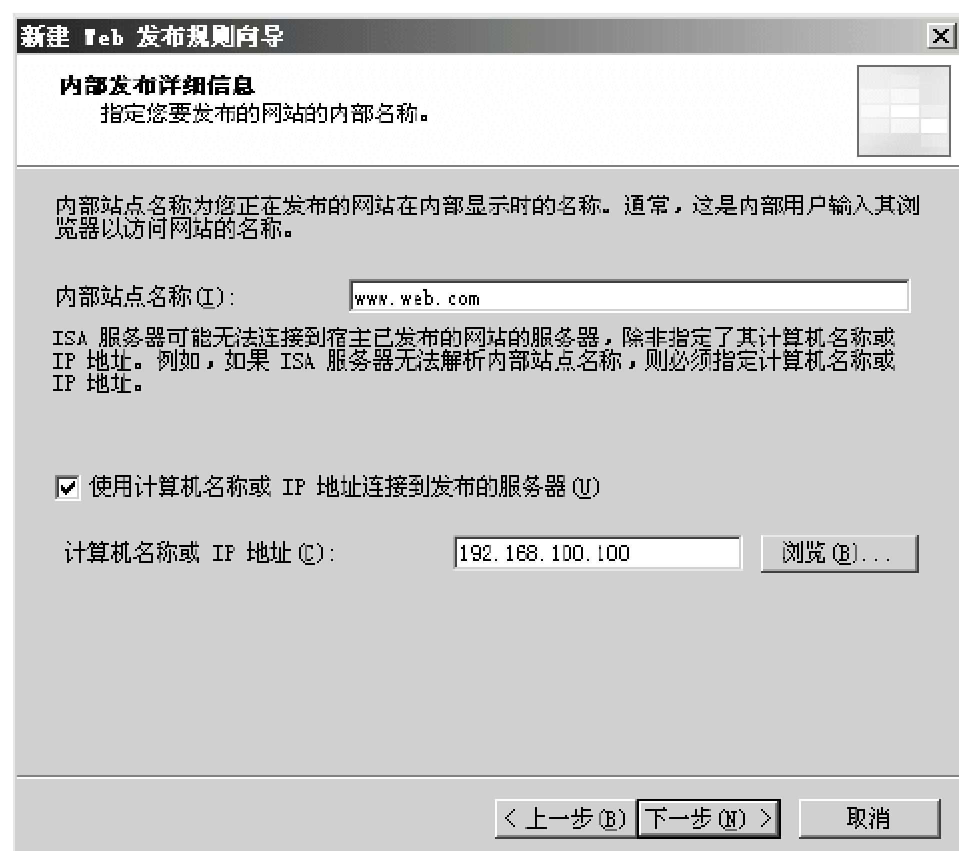


图 20-81 【内部发布详细信息】对话框

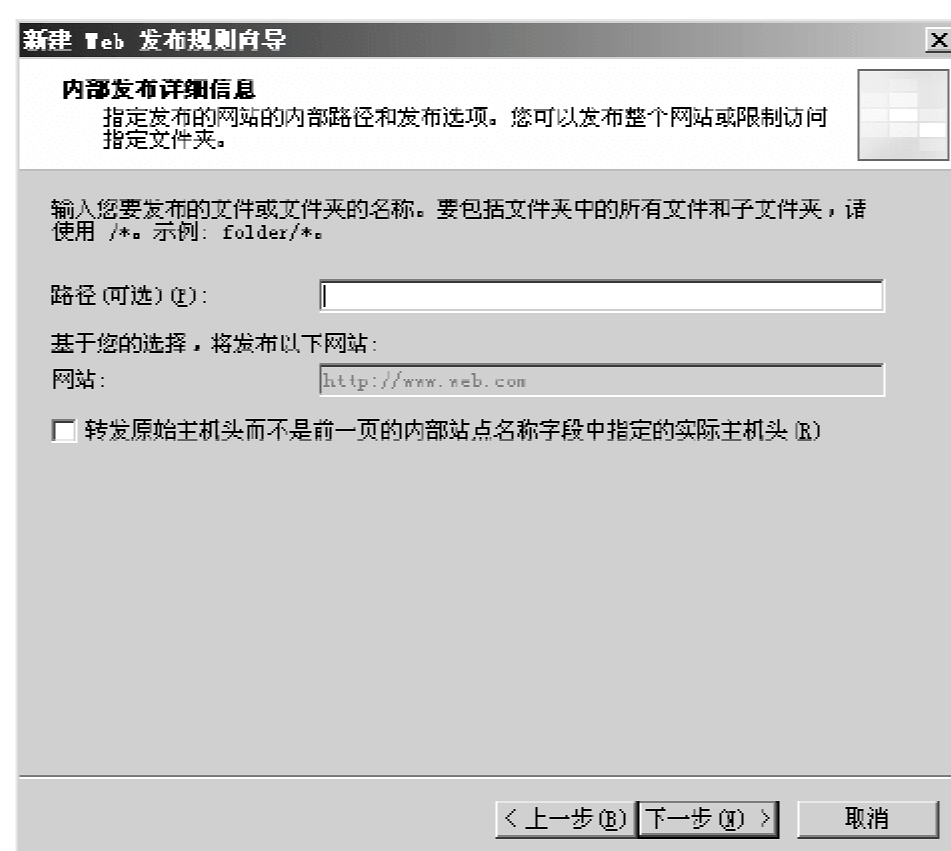


图 20-82 内部发布网站信息补充

08 弹出【公共名称细节】对话框，如图 20-83 所示，在【公用名称】文本框中输入公网访问企业网站使用的域名，该域名需要在域名注册机构注册，本实例使用“www.Web .com”为例讲解，单击【下一步】按钮。

09 弹出【选择 Web 侦听器】对话框，如图 20-84 所示，单击【新建】按钮。



图 20-83 【公共名称细节】对话框

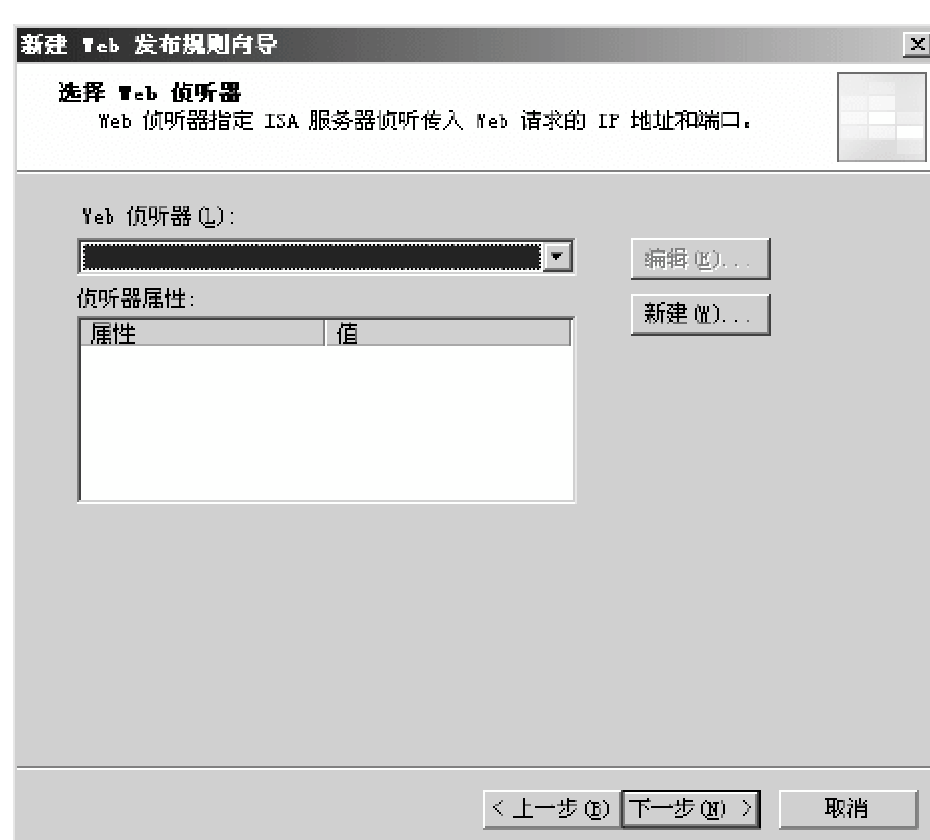


图 20-84 【选择 Web 侦听器】对话框

10 弹出【新建 Web 侦听器定义向导】对话框，如图 20-85 所示，在【Web 侦听器名称】文本框中输入“外部 WEB 访问”，单击【下一步】按钮。

11 弹出【客户端连接安全设置】对话框，由于本实例不采用 SSL 安全连接，所以选中【不需要与客户端建立 SSL 安全连接】单选按钮，如图 20-86 所示，单击【下一步】按钮。

12 弹出【Web 侦听器 IP 地址】对话框，如图 20-87 所示，选择侦听 Web 访问请求的端口或地址段，选中【外部】复选框，单击【下一步】按钮。

13 弹出【身份验证设置】对话框，如图 20-88 所示，选择【没有身份验证】选项，单击【下一步】按钮。

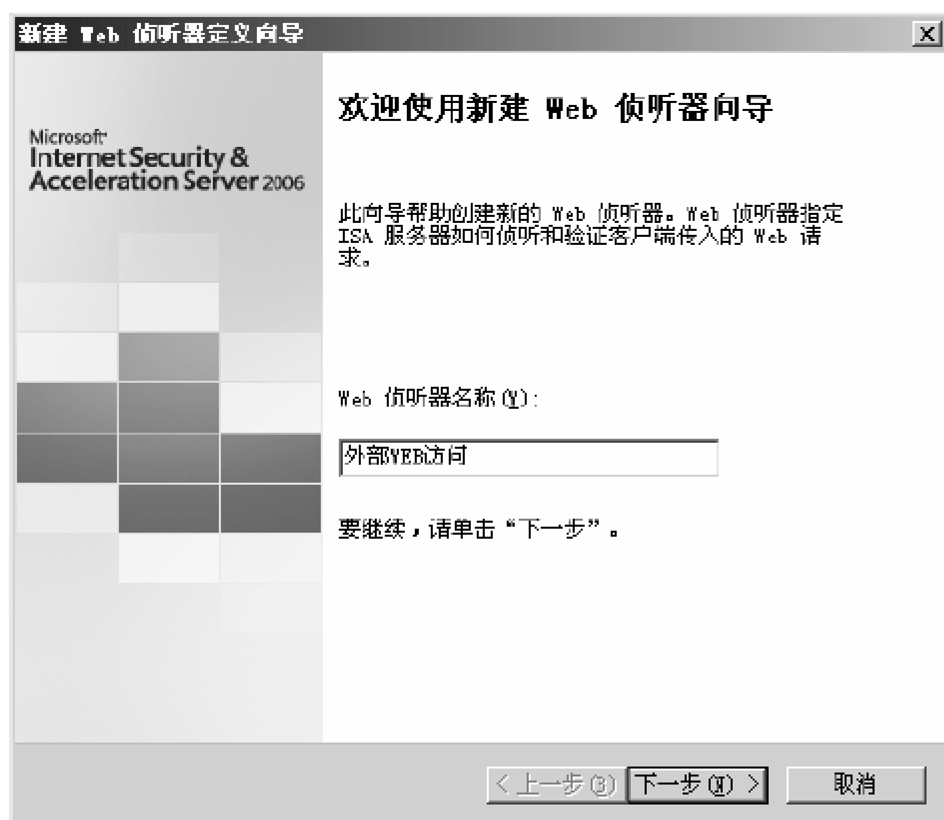


图 20-85 【新建 Web 侦听器定义向导】对话框

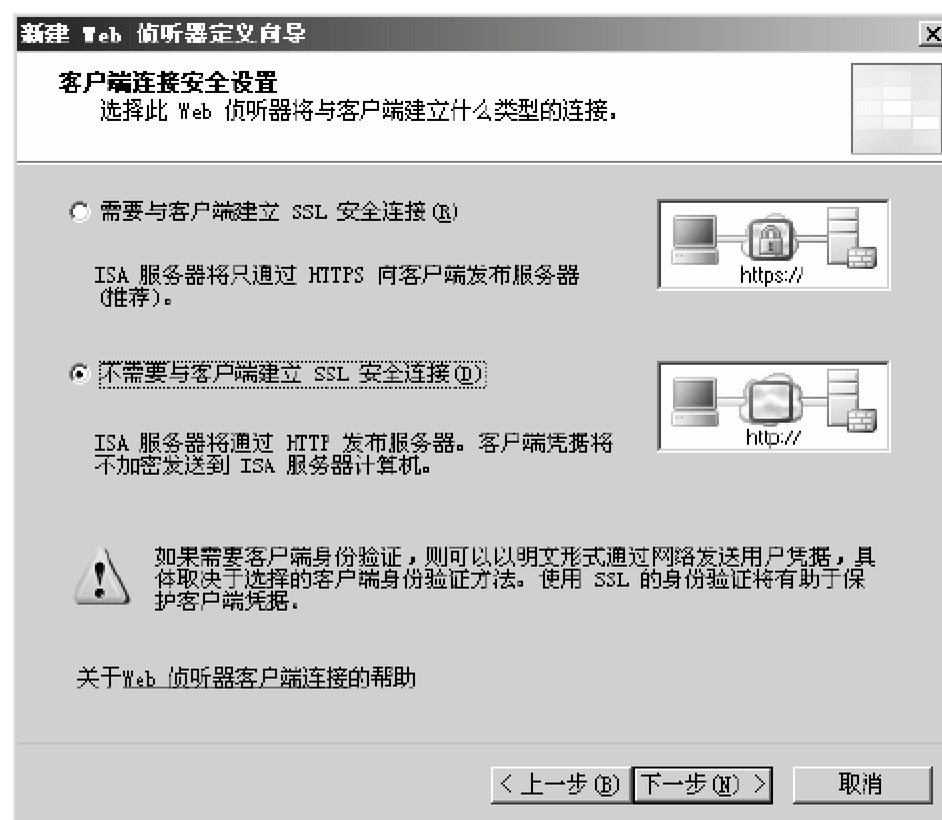


图 20-86 【客户端连接安全设置】对话框

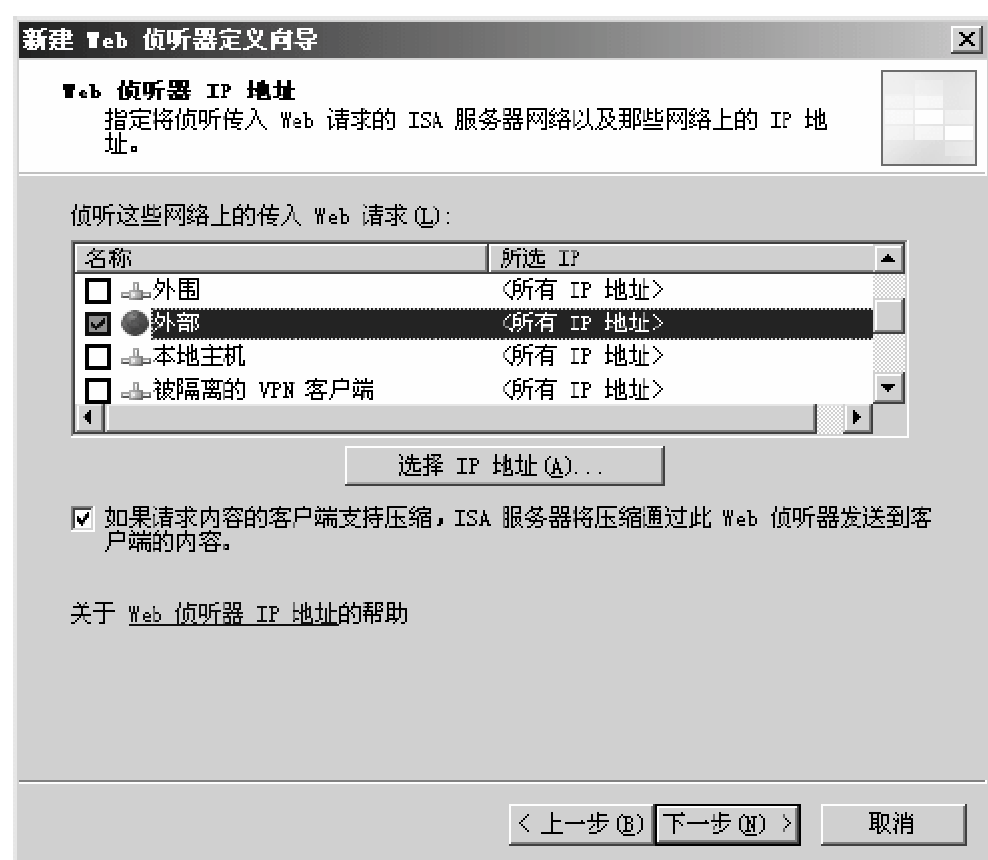


图 20-87 【Web 侦听器 IP 地址】对话框

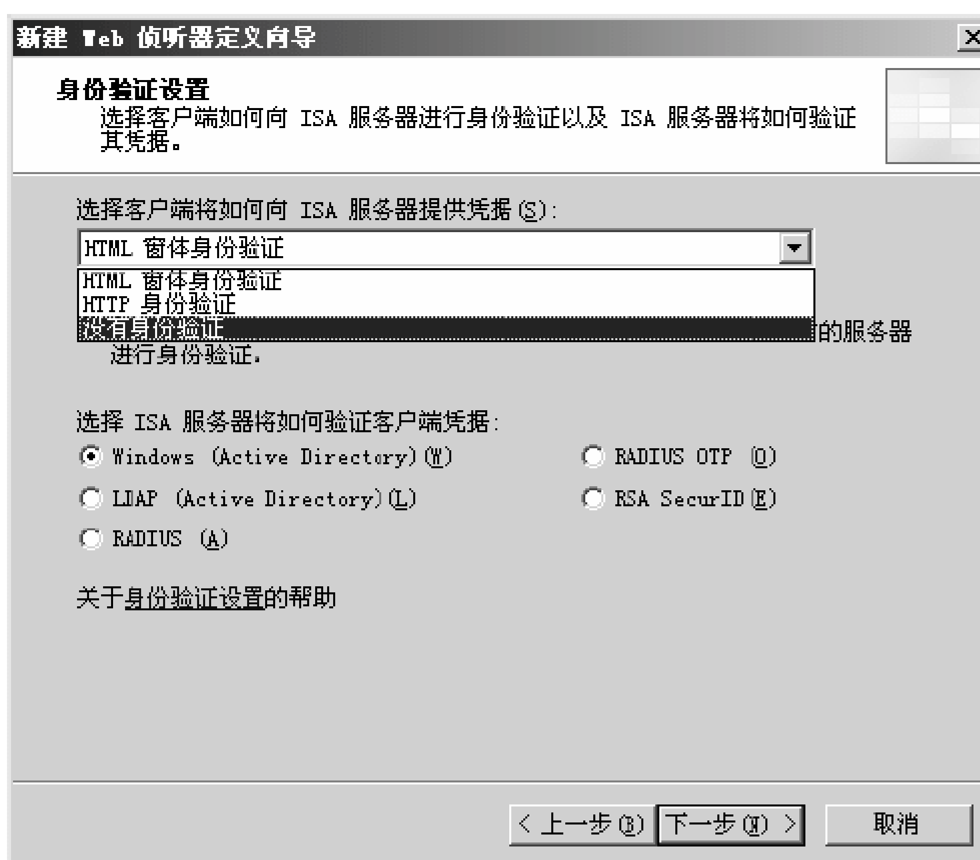


图 20-88 【身份验证设置】对话框

14 弹出【单一登录设置】对话框，本实例中没有身份认证问题，不做操作，如图 20-89 所示，单击【下一步】按钮。

15 Web 侦听器配置完成，如图 20-90 所示，在弹出的对话框中显示了详细配置内容，单击【完成】按钮。

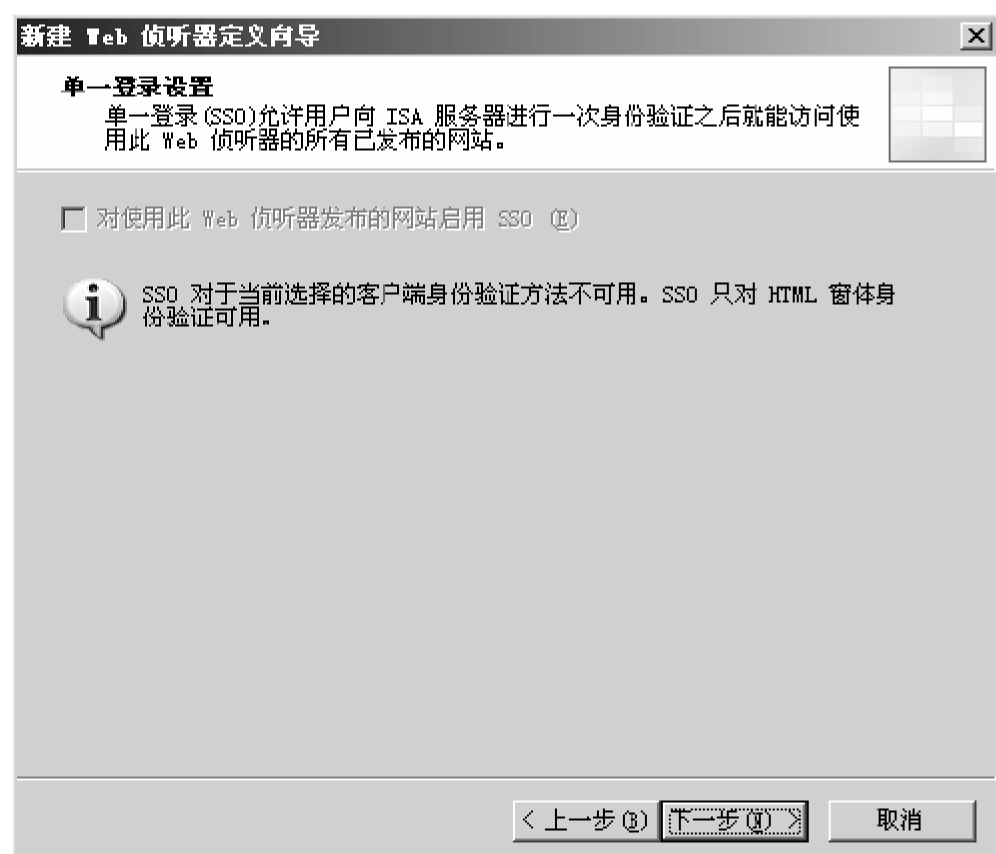


图 20-89 【单一登录设置】对话框

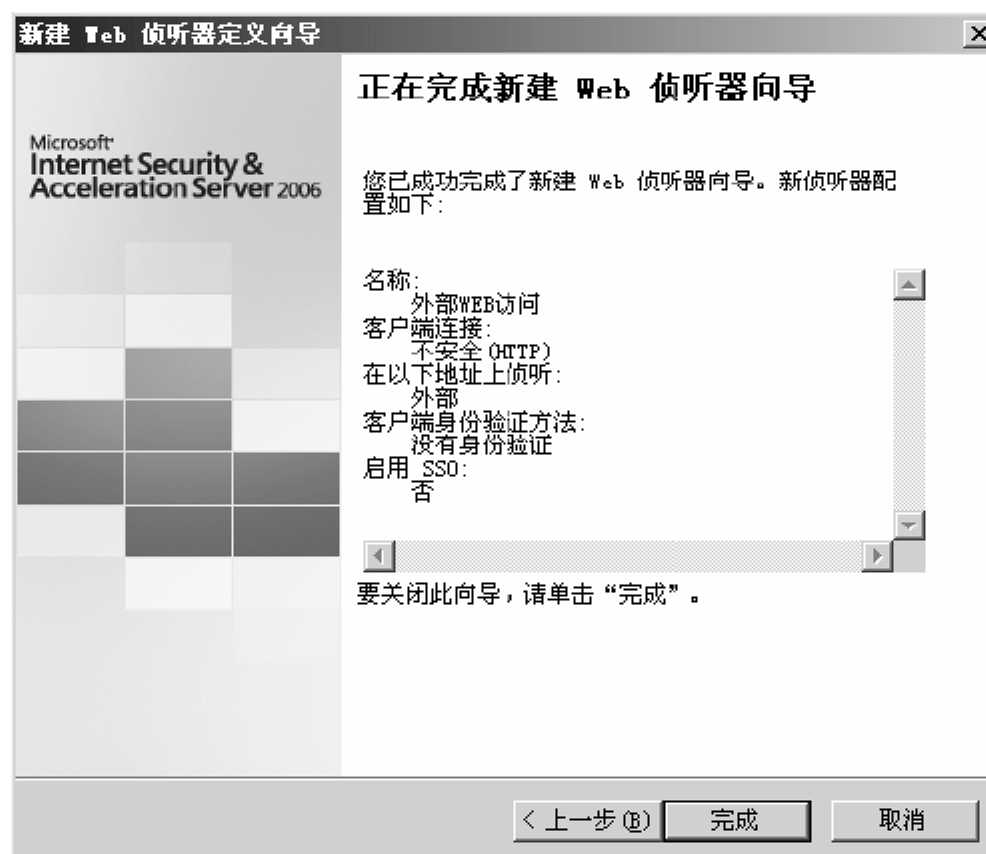


图 20-90 完成新建 Web 侦听器向导

16 返回【选择 Web 侦听器】对话框，如图 20-91 所示，新建 Web 侦听器已被应用，单击【下一步】按钮。

17 弹出【身份验证委派】对话框，因为本实例不配置身份验证，所以选择【无委派，客户端无法直接进行身份验证】选项，如图 20-92 所示，单击【下一步】按钮。



图 20-91　【选择 Web 侦听器】对话框

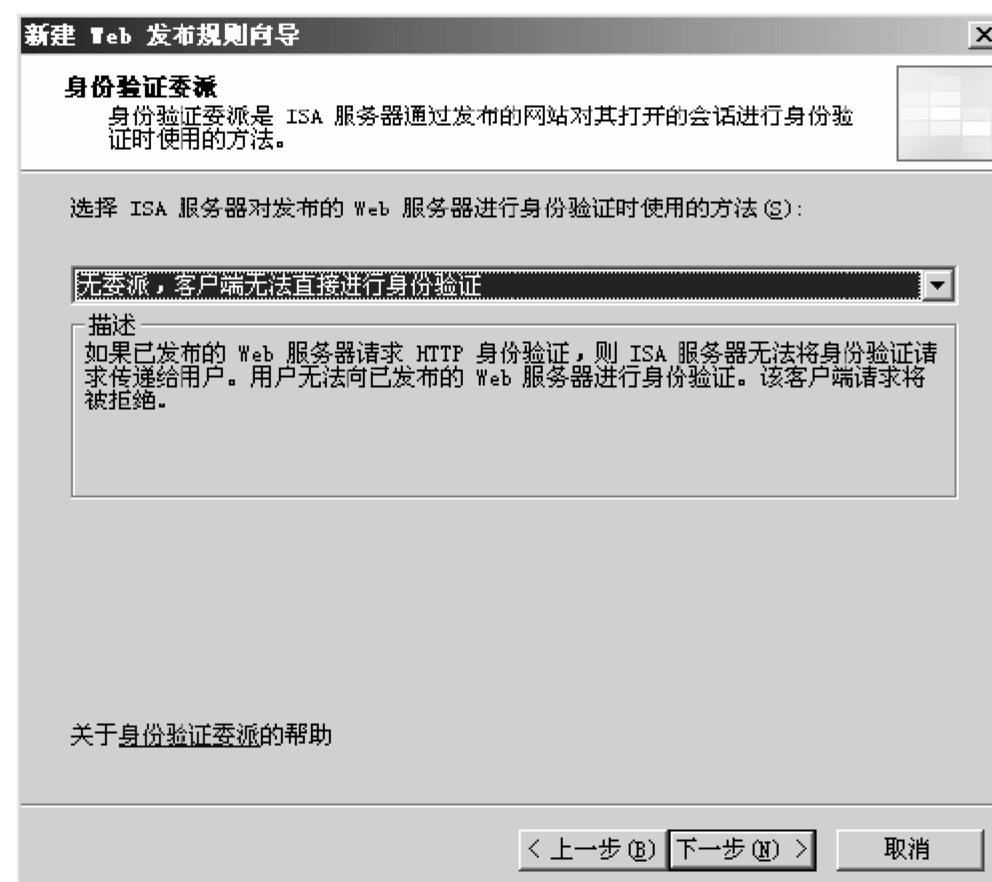


图 20-92　【身份验证委派】对话框

18 弹出【用户集】对话框，如图 20-93 所示，默认将此规则应用到所有用户的请求，单击【下一步】按钮。

19 Web 服务器发布配置完成，如图 20-94 所示，在弹出的对话框中显示了详细的配置信息，单击【完成】按钮。



图 20-93　【用户集】对话框

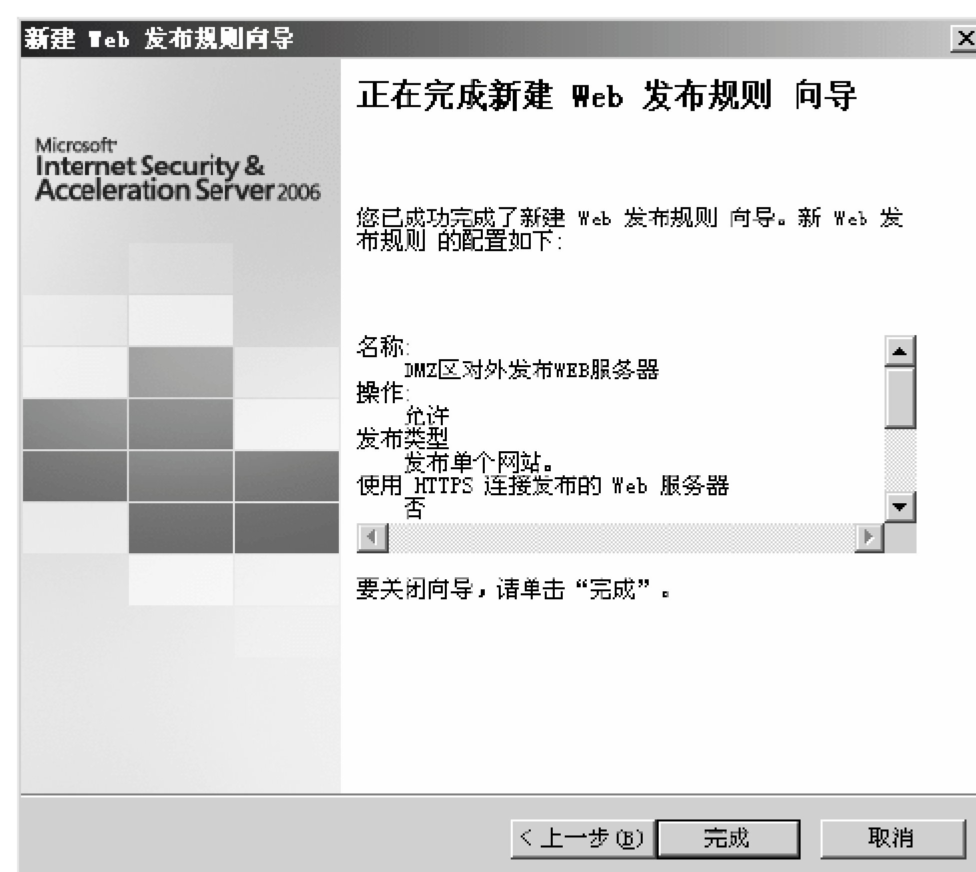


图 20-94　完成新建 Web 发布规则向导

20 返回程序主界面，如图 20-95 所示，单击【应用】按钮使配置生效。



图 20-95　应用 Web 网站发布配置


提 示

配置发布 Web 服务器时，内网和外网访问使用的域名必须是可以被 DNS 服务器解析到的。

20.4.2　ISA 防火墙安全发布邮件服务器

很多企业为了工作方便都会配备企业邮箱，为了保证企业邮箱在内外网都可以使用，这就需要防火墙发布邮件服务器。

邮件服务器的发布步骤如下。

01 在程序主界面右侧【任务】选项卡选择【发布邮件服务器】选项，如图 20-96 所示。



图 20-96　新建发布邮件服务器任务

02 弹出【新建邮件服务器发布规则向导】对话框，如图 20-97 所示，在【邮件服务器发布规则名称】文本框中输入“企业邮件服务器”，单击【下一步】按钮。

03 弹出【选择访问类型】对话框，如图 20-98 所示，选中【客户端访问：RPC、IMAP、POP3、SMTP】单选按钮，单击【下一步】按钮。

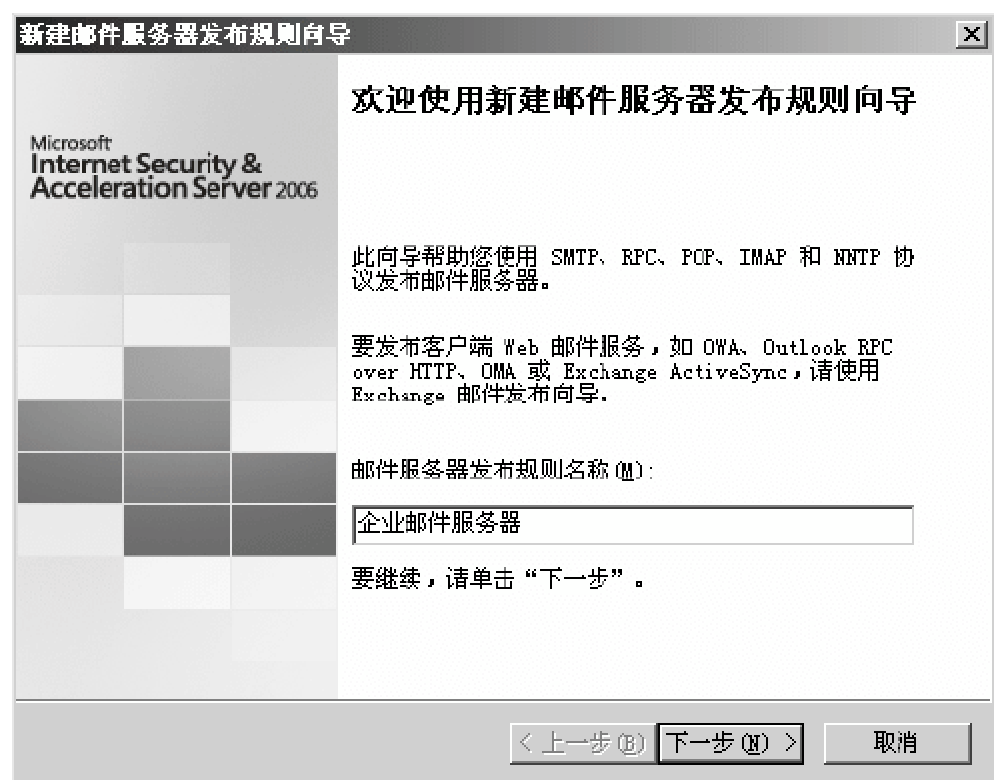


图 20-97 【新建邮件服务器发布规则向导】对话框

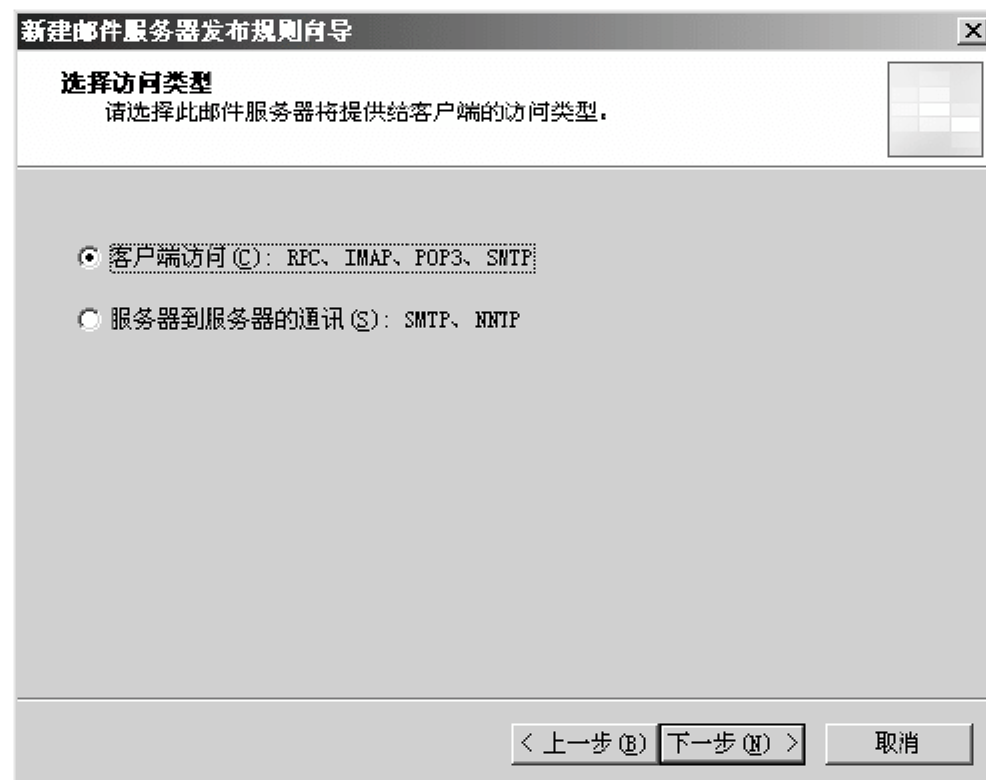


图 20-98 【选择访问类型】对话框

04 弹出【选择服务】对话框，常用邮件服务有 POP3、SMTP、IMAP4，“secure port”意思是安全端口，如果访问邮件时使用认证技术可以选择右侧三项复选框，本实例选择左侧四项复选框，如图 20-99 所示，单击【下一步】按钮。

05 弹出【选择服务器】对话框，如图 20-100 所示，在【服务器 IP 地址】文本框中输入 DMZ 区邮件服务器的 IP 地址，本实例采用“192.168.100.100”地址，单击【下一步】按钮。

06 弹出【网络侦听器 IP 地址】对话框，如图 20-101 所示，在【侦听来自这些网络的请求】选项列表中选中【外部】复选框，单击【下一步】按钮。

07 配置完成，如图 20-102 所示，在弹出的对话框中显示了发布邮件服务器的配置信息，单击【完成】按钮。

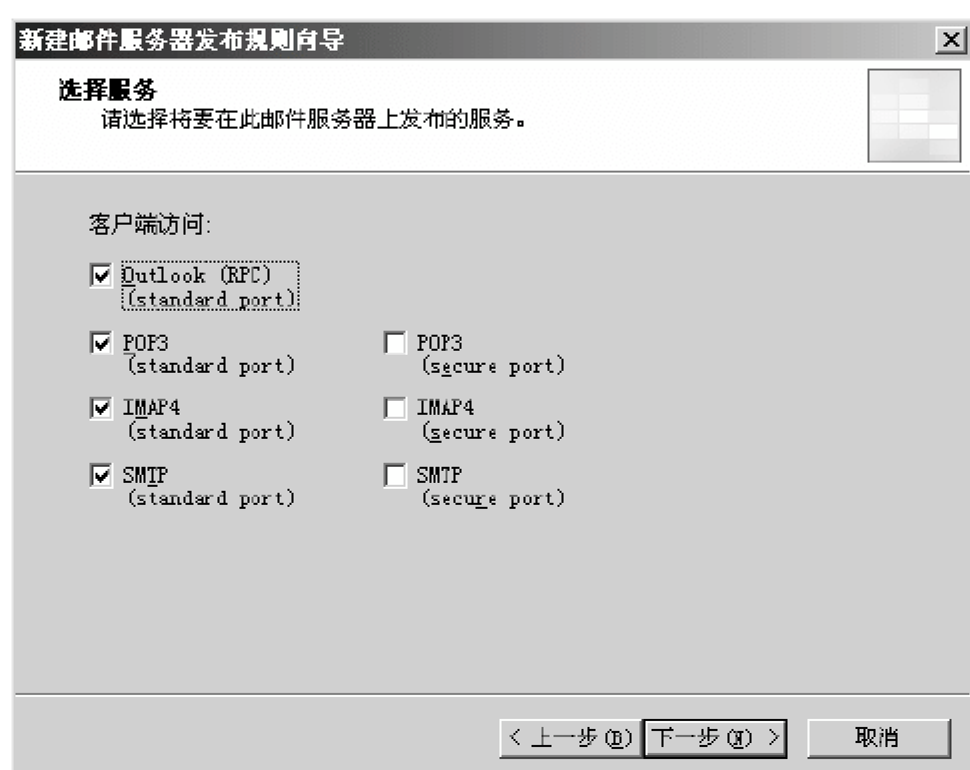


图 20-99 【选择服务】对话框

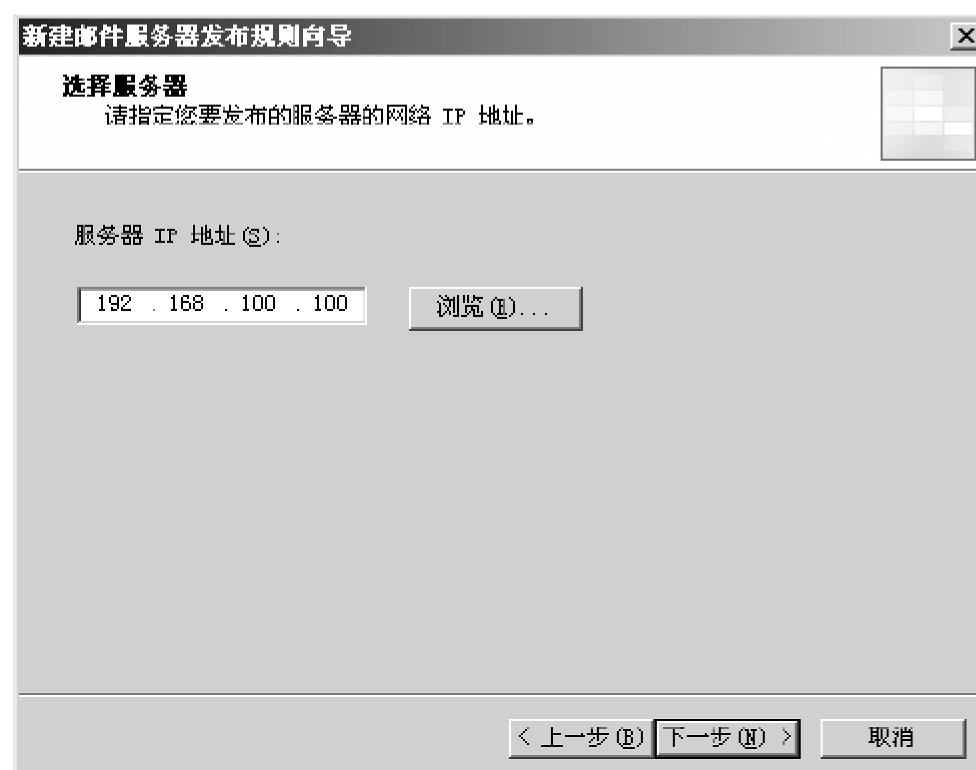


图 20-100 【选择服务器】对话框

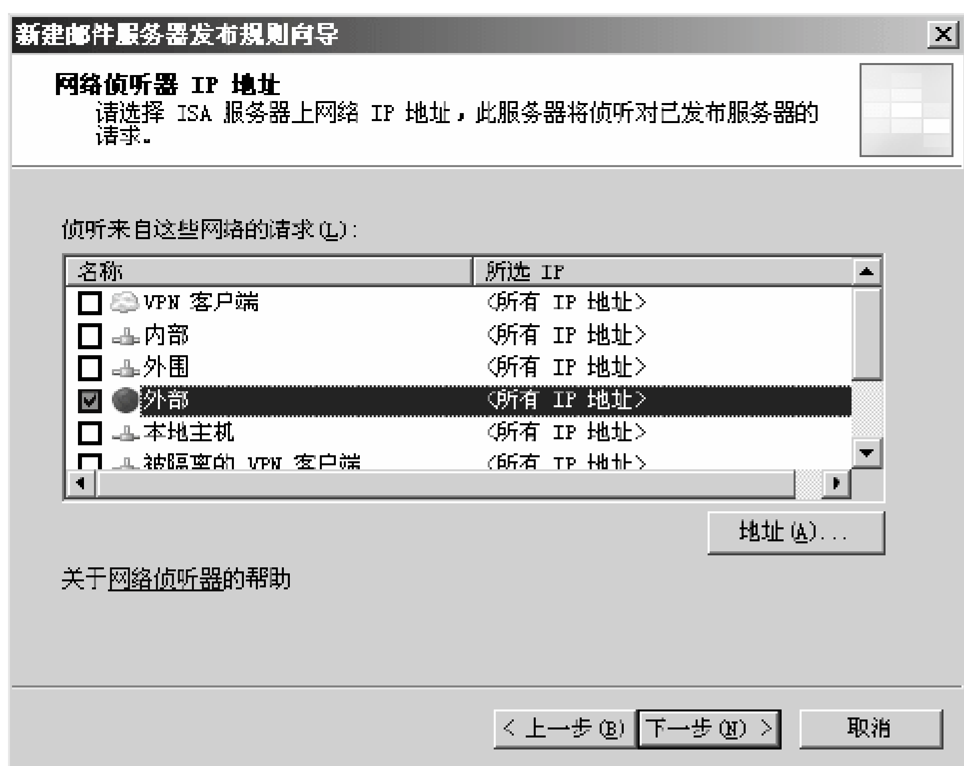


图 20-101 【网络侦听器 IP 地址】对话框

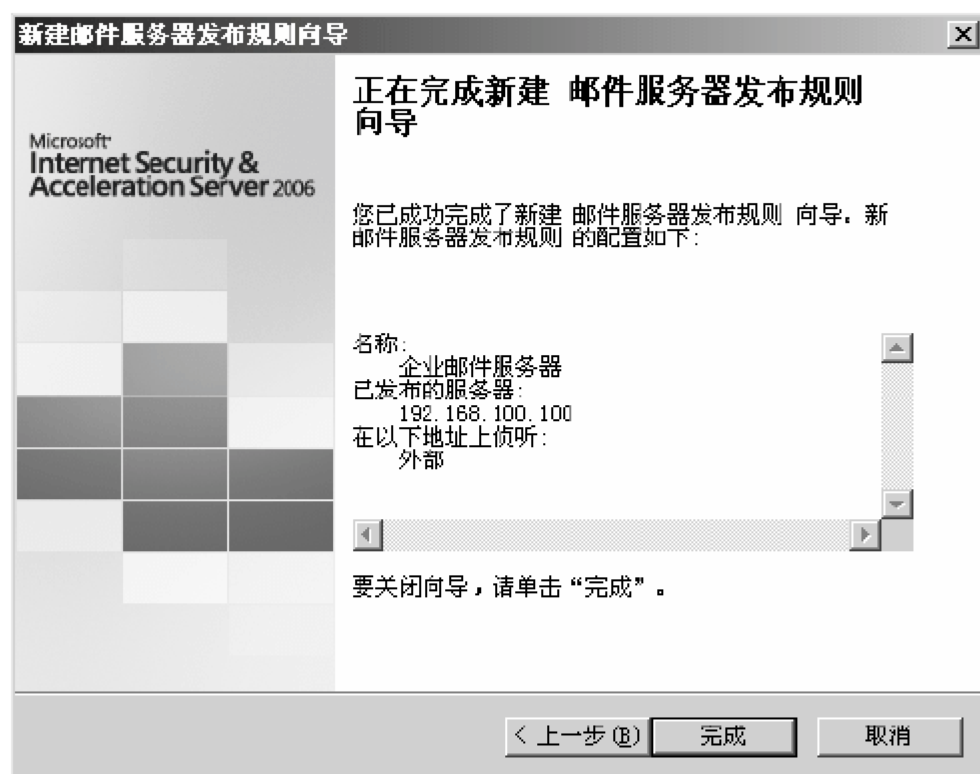


图 20-102 完成新建邮件服务器发布规则向导

08 返回程序主界面，如图 20-103 所示，单击【应用】按钮使配置生效。



图 20-103 应用邮件服务器发布配置

20.4.3 ISA 防火墙安全发布其他服务器

使用 ISA 防火墙发布其他服务器的操作步骤类似，以 DNS 服务器的发布为例，其具体的操作步骤如下。

01 打开程序主界面，如图 20-104 所示，在右侧【任务】选项卡中选择【发布非 Web 服务器协议】选项。

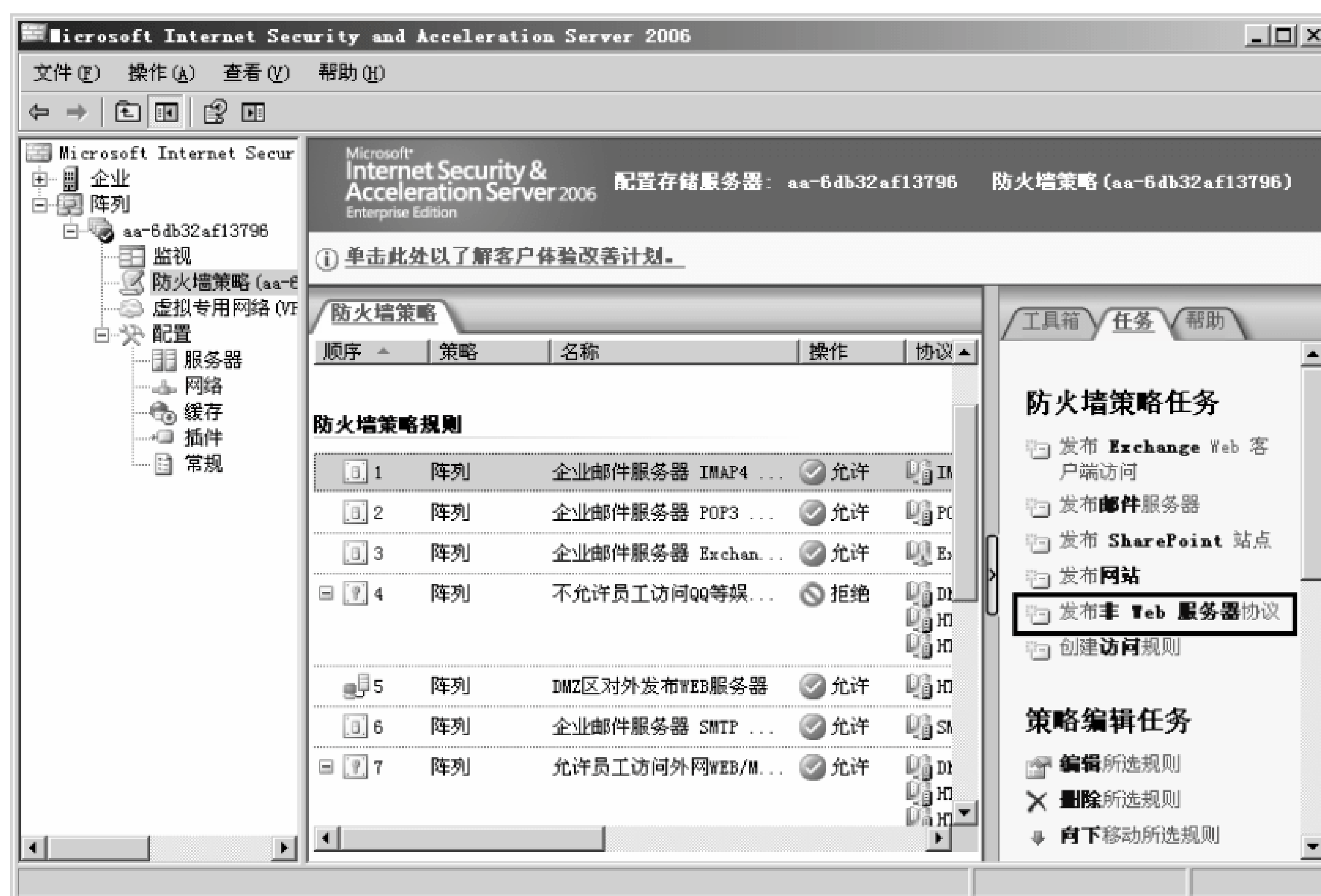


图 20-104　创建发布非 Web 服务器协议任务

02 弹出【新建服务器发布规则向导】对话框，如图 20-105 所示，在【服务器发布规则名称】文本框中输入“企业 DNS 服务器发布”，单击【下一步】按钮。

03 弹出【选择服务器】对话框，如图 20-106 所示，在【服务器 IP 地址】文本框中输入 DNS 服务器的 IP 地址“192.168.100.100”，单击【下一步】按钮。

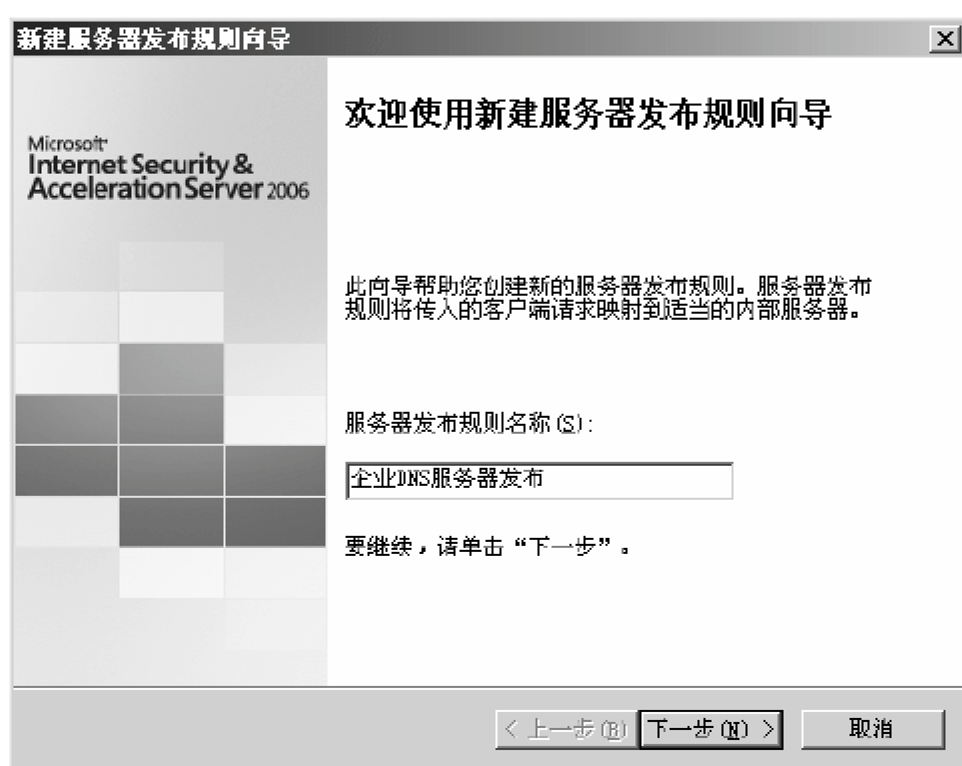


图 20-105　【新建服务器发布规则向导】对话框

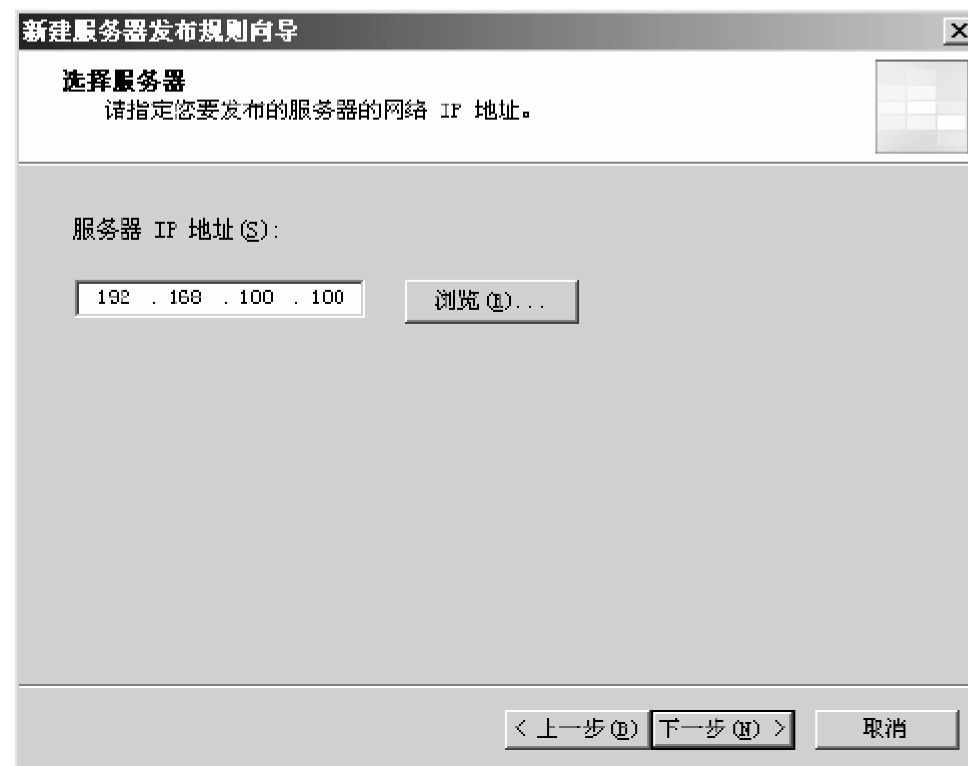


图 20-106　【选择服务器】对话框

04 弹出【选择协议】对话框，如图 20-107 所示，在【选择的协议】下拉列表框中选择【DNS 服务器】选项，单击【下一步】按钮。

05 弹出【网络侦听器 IP 地址】对话框，如图 20-108 所示，在【侦听来自这些网络的请求】选项列表中选择【外部】选项，单击【下一步】按钮。



图 20-107 【选择协议】对话框

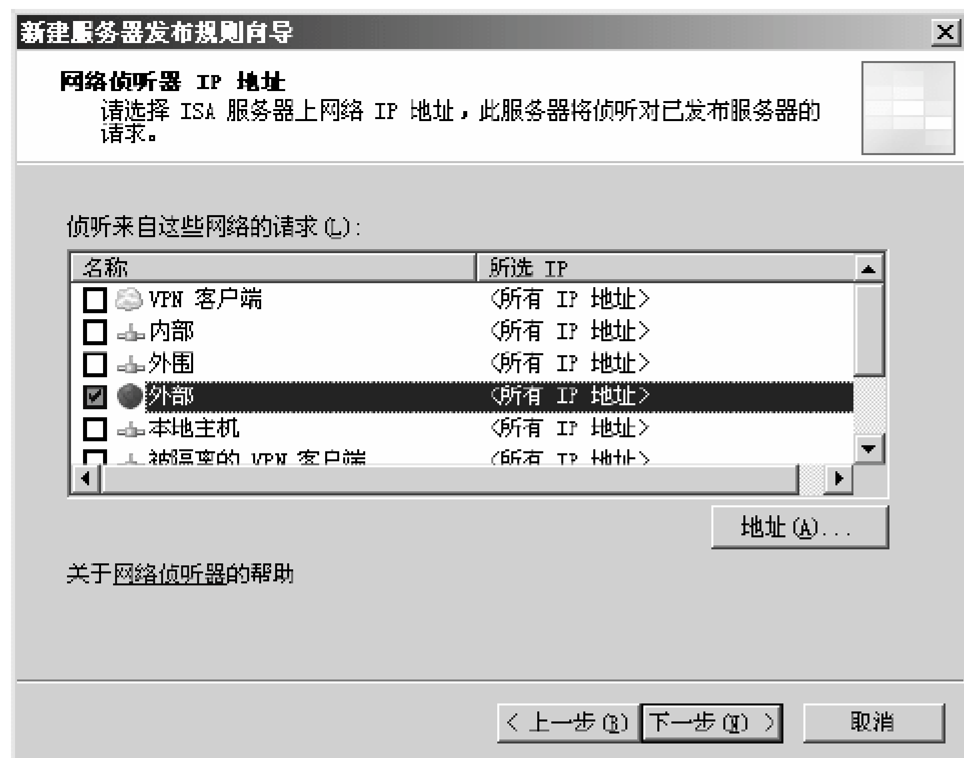


图 20-108 【网络侦听器 IP 地址】对话框

06 配置完成，如图 20-109 所示，在弹出的对话框中显示了新发布 DNS 服务器的配置信息，单击【完成】按钮。

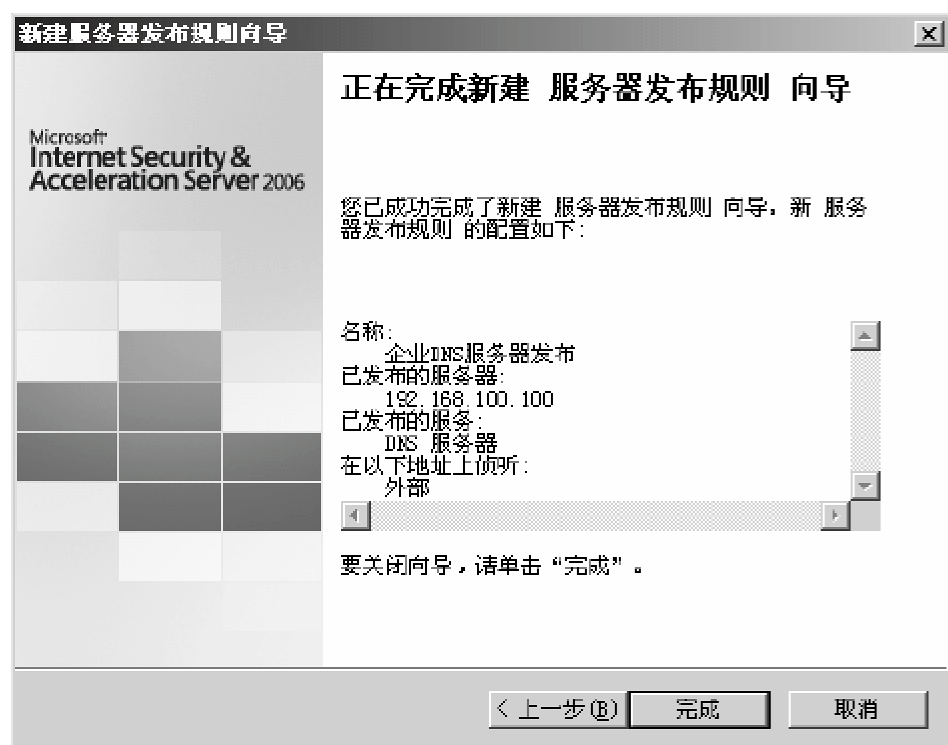


图 20-109 完成新建服务器发布规则向导

07 返回程序主界面，如图 20-110 所示，单击【应用】按钮使配置生效。



图 20-110 应用服务器发布配置

20.5 专家答疑

（1）如果企业使用了出口防火墙部署，个人计算机上还有必要配置防火墙吗？

答：企业防火墙是用来防护外网攻击的，对于内网产生的攻击防护能力很弱。所以在企业中每一台主机都需要开启个人防火墙，以防护局域网的病毒或木马攻击。同时个人防火墙还可以防止非法链接。

（2）企业防火墙的访问策略应当按照什么样的原则进行配置？

答：一般默认规则要选择拒绝所有流量，其他流量应该遵循以下两条原则。

①简单实用。防火墙属于较为复杂的安全设备，其涉及的技术比较广泛，而很多网络管理人员技术水平有限，很难驾驭防火墙。如果配置不慎，出现了配置错误，没有很好的经验恢复起来会很吃力。所以在配置访问规则的时候，能简化的尽量简化，越简单的实现方式，越容易理解和使用。而且是设计越简单，越不容易出错，防火墙的安全功能越容易得到保证，管理也越可靠和简便。简单可以，但是要尽量禁止一切无用流量的通信。

防火墙的安全功能很多，但是这些功能并不是所有应用环境都需要，配置时要结合企业需求，不必要的功能尽力使用默认配置，否则会大大增强配置难度，而且还可能因配置不当而引起新的安全漏洞。

②结合全网安全架构需求。很多用户配置防火墙时，只是看到了防火墙本身的防护，配置几条访问策略就了事了。而网络需要全面的、多层次的深层防御战略体系才能实现真正的安全。要与入侵检测、网络加密认证、病毒查杀等多种安全措施相结合，构建多层次多角度的安全体系。